3/2017

Datenschutz Nachrichten

40. Jahrgang
ISSN 0137-7767
12,00 Euro



40 Jahre DVD

■ 40 Jahre im Verein ■ Die Entwicklung der DVD in den letzten zehn Jahren ■ Grußworte ■ Controlling der IT-Sicherheit ■ Kuriositäten in der [Datenschutz-]Gesetzgebung ■ Wenn aus Spiel Wirklichkeit wird ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Donnerstag, 01. Februar 2018
Redaktionsschluss DANA 1/2018

Samstag, 24. Februar 2017
DVD-Vorstandssitzung
Bonn, Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 20. April 2018, 18:00 Uhr
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Samstag, 21. April 2018
DVD-Vorstandssitzung
Bielefeld,
Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
40. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frank Spaeing, Riko Pieper
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
AdobeStock, ClipDealer

Editorial

40 Jahre DVD! Anlässlich dieses Jubiläums beginnen wir dieses Heft mit einem Rückblick auf diese 40 Jahre. Ein erster Artikel von Heinz Alenfelder und Thilo Weichert beschreibt die ersten ca. 20 DVD-Jahre. Ein zweiter (deutlicher kürzerer) Rückblick von Heinz Ahlenfelder gibt einen persönlichen Rückblick auf 40 Jahre DVD. Ergänzt werden diese beiden Artikel vom aktuellen Vorstandsvorsitzenden, Frank Spaeing, um die aktuellen Themen und Entwicklungen der letzten Jahre.

Danach folgen Grußbotschaften von teils langjährigen Weggefährten, die wir in alphabetischer Reihenfolge wiedergeben. Bei näherer Betrachtung der Absender der Grußbotschaften fällt auf, dass hier neben der Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder) und besagten Wegbegleitern auch andere Bürgerrechtsorganisationen bzw. Datenschutzvereine vertreten sind, die durchaus ähnliche Interessen verfolgen wie die DVD.

Wir sehen uns also nicht als Konkurrenz, sondern als Ergänzung mit jeweils unterschiedlichen Schwerpunkten – und Möglichkeiten. Ein Vorstandsmitglied einer anderen Organisation sagte auf deren Mitgliederversammlung in diesem Jahr: „Wir sind der DVD dankbar für die klare, kritische Stellungnahme zum neuen BDSG, die wir selbst so deutlich nicht formulieren können.“ Kann es ein besseres Kompliment geben?

Natürlich kommen in diesem Heft auch die Fachbeiträge nicht zu kurz. Es gibt derer drei in dieser DANA-Ausgabe:

Der erste Artikel von Dr. Bernd Schütze befasst sich mit dem Controlling der IT-Sicherheit unter Berücksichtigung von Art. 32 Datenschutz-Grundverordnung. Der nächste Artikel von Riko Pieper beschreibt anhand von elf Beispielen Kuriositäten im Datenschutzrecht, wobei manche dieser Beispiele nur kurios aber harmlos sind, andere jedoch ernste und teilweise aktuelle Probleme beschreiben. Die jeweiligen Konklusionen wurden teilweise mit einem Augenzwinkern geschrieben und dürfen nicht zu wörtlich genommen werden. Ergänzend zu den reinen Datenschutzthemen folgt der Artikel „Wenn aus Spiel Wirklichkeit wird“ von Ute Bernhardt zu Potenzialen kollaborativer Augmented Reality.

Anschließend haben wir Ihnen noch eine Pressemitteilung der Berliner BfDI zum „Artikel-Gesetz für mehr Sicherheit und mehr Datenschutz in Berlin“, eine Rede des Bundesjustizministers Maas zum Zusammenleben in der digitalen Gesellschaft sowie einen Leserbrief von Patrick Breyer mit einer Replik durch Vorstandsmitglied Thilo Weichert in dieses Heft gepackt.

Abgerundet wird dieses Heft wie gewohnt durch die Datenschutznachrichten aus dem In- und Ausland, zu technischen Datenschutzthemen sowie zur Rechtsprechung und durch Buchbesprechungen.

Wir wünschen Ihnen in diesen interessanten und (mitunter auch) stürmischen Zeiten eine angenehme Lektüre

Frank Spaeing und Riko Pieper

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD, alenfelder@datenschutzverein.de

Ute Bernhardt
Mitglied im wissenschaftlichen Beirat des FIfF e. V. sowie im Netzwerk-Datenschutzexpertise.

Riko Pieper
Vorstandsmitglied in der DVD, pieper@datenschutzverein.de

Dr. Bernd Schütze
Langjähriger Experte im Bereich Datenschutz und IT-Sicherheit,
schuetze@medizin-informatik.org

Frank Spaeing
Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Die ersten Jahre der DVD

Dieser Artikel von Heinz Alenfelder und Thilo Weichert basiert auf einem Beitrag für die Zeitschrift "vorgänge" – Zeitschrift für Bürgerrechte und Gesellschaftspolitik; Heft 4, Dezember 1999, Nr. 148, Der vermessene Mensch.

Kleine Geschichte

Datenschutz ist ein Bürgerrecht. Es ist daher kein unsinniges Unterfangen nach dem Schicksal einer Bürgerrechtsorganisation zu fragen, um über den Zustand dieses Bürgerrechts etwas zu erfahren. Dass Datenschutz – in der Juristensprache das Recht auf informationelle Selbstbestimmung – als Bürgerrecht etabliert ist, verdanken wir vor allem der Volkszählungsentscheidung des Bundesverfassungsgerichts von 1983. Dass es zu dieser Entscheidung gekommen ist, verdanken wir aber der öffentlichen Diskussion um den Datenschutz und damit den Personen und Organisationen, die sich in dessen Interesse engagiert haben.

Datenschutz wurde nicht immer als Bürgerrecht für jede und jeden verstanden. Zwar wurde die moderne Datenschutzdebatte in den USA schon im Jahr 1890 mit einem Aufsatz von Warren und Brandeis über ein allgemeines „Right to Privacy" losgetreten. In Deutschland wurde das allgemeine Persönlichkeitsrecht bis in die jüngste Vergangenheit vor allem als ein Recht der Eliten angesehen.

Das Recht am eigenen Bild z.B. wurde 1907 in das Kunst- und Urhebergesetz hineingeschrieben, weil ein Journalist als früher Paparazo die Leiche von Bismarck fotografierte und dieses Bild veröffentlichte. Bei den Gerichtsentscheidungen zum Persönlichkeitsrecht ging es zunächst um Klagen von Prominenten gegen die nicht autorisierte Veröffentlichung ihres Namens oder Bildes für Werbe- oder sonstige kommerzielle Zwecke (z.B. Herrenreiterfall, Soraya). Die Popularisierung dieses Rechts kam erst mit dem Erlass der ersten Datenschutzgesetze in den 70er Jahren.

Die Gründung der Deutschen Vereinigung für Datenschutz Ende 1977 erfolgte nicht als medialer Paukenschlag, sondern als Versuch, ein kleines zartes Pflänzchen hochzuziehen. Das erste Datenschutzgesetz, nicht nur Deutschlands, sondern weltweit, war schon 1970 vom Hessischen Landtag verabschiedet worden. Auch auf Bundesebene hatten wir inzwischen ein „Gesetz zum Schutz vor Missbrauch personenbezogener Daten"- das Bundesdatenschutzgesetz (BDSG), welches im Januar 1977 verabschiedet wurde und zum darauf folgenden Jahreswechsel in Kraft trat. Die DVD-Gründung war ein Reflex auf diese politische Entwicklung, nicht deren Auslöser. Einige, aus der gemeinsamen Tätigkeit bei bzw. mit der Gesellschaft für Mathematik und Datenverarbeitung (GMD) in Bonn befreundete und bekannte Mitstreiter, gründeten den Verein.

Dieser sollte die "datenschutzbezogenen Interessen der Bürger sowie die Position der Datenschutzbeauftragten in den Betrieben" stärken. Ziele waren die Herausgabe einer Fachzeitschrift, die Durchführung von Schulungen und die Mitgliederberatung in Datenschutzfragen. Die AktivistInnen der ersten Tage sind teilweise heute noch im Datenschutzgeschäft tätig. Doch haben sie sich fast durchgängig – viele im Wissenschaftsbetrieb, einige auch in der „freien" Wirtschaft – etabliert und dabei zumeist der DVD – auch bei Bewahrung einer freundlicher Grundeinstellung – den Rücken zugewandt. August 1978 erschien die erste Ausgabe der eigenen Zeitschrift – der Datenschutz Nachrichten (DANA). Die Position war – wie die der DVD – von Anfang an bürgerrechtlich, staatskritisch und linksliberal. So fragte die erste Überschrift der DANA, ob das neue Bundesdatenschutzgesetz (BDSG) nicht ein „Ermächtigungsgesetz für staatliche Informationszentralen" sei und kam auch gleich zu der Antwort, dass hier ein Schutzgesetz in sein Gegenteil verkehrt worden sei. Ein Heft der DANA kostete damals DM 5,50; inzwischen sind es DM 12,50.

Dabei ist nicht zu verkennen, dass sich der Inhalt – zumindest quantitativ und auch Dank moderner Informationstechnologie – vervielfacht hat. In den über zwanzig Jahren hat die zunächst sechsmal, jetzt viermal jährlich erscheinende DANA immer zeitnah über datenschutzrelevante Entwicklungen und über die DVD-Arbeit berichtet. Inzwischen gibt es eine Vielzahl von Datenschutzzeitschriften mit vielen juristischen und technischen Informationen; die DANA ist die einzige geblieben, die einen politischen, engagierten und bürgerrechtlichen Anspruch hat und verwirklicht.

Struktur und Arbeitsweise

Die Keimzelle der DVD lag in Bonn – und damit am Regierungssitz der Bundesrepublik Deutschland. Ein wissenschaftlicher Beirat sollte die Verbandsarbeit von Anfang an kritisch begleiten. Doch diese Struktur erwies sich für eine bundesweite Organisation mit ca. 200 Mitgliedern langfristig als nicht überlebensfähig.

Wenn sich im Rahmen des Widerstandes gegen die Volkszählung 1983 auch die in der ganzen Republik verbreiteten Kontakte und Regionalgruppen als wichtig erwiesen, so konzentrierten sich die Aktivitäten doch vorrangig auf die Vorstandsarbeit, die Erstellung der DANA und auf bundesweite Koordination. Sie ging von Bonn aus, wo auch die Geschäftsstelle untergebracht war. Die Vorstände nahmen ihre Aufgaben immer ehrenamtlich wahr. Auch die Geschäftsstellenarbeit war lange Zeit ehrenamtlich. Erst 1985 war es möglich, die Geschäftsstellentätigkeit, wenn auch nur in sehr beschränktem Umfang, zu entlohnen.

Die Finanzierung des Vereins basierte immer vor allem auf der Zahlung von Mitgliedsbeiträgen, darüber hinaus auch auf Spenden sowie auf Überschüssen aus Veranstaltungen und Seminaren. Da die DVD als gemeinnützig anerkannt ist, können Spenden steuerlich abge-

setzt werden. Bei den Preisen – nicht nur der DANA – versucht die DVD seit über 20 Jahren Bürgerfreundlichkeit zu wahren. Die Mitgliedsbeiträge bewegen sich heute mit 80 DM bzw. ermäßigt mit 35 DM pro Jahr für Einzelpersonen und 150 DM für Organisationen und Firmen in einem sehr vertretbaren Rahmen.

Die Tätigkeit der DVD hat eine Vielzahl von Facetten: Die Beratungsersuchen von BürgerInnen können nur in einem eingeschränkten Umfang befriedigt werden. Mitglieder haben einen Anspruch auf Unterstützung. Zumeist ist es aber wegen der Vielzahl der externen Anfragen nur möglich, auf die zuständigen Datenschutzbehörden im Bund und in den Ländern zu verweisen. Hauptschwerpunkt der DVD-Arbeit ist die bürgerrechtliche Begleitung der Datenschutzentwicklung in Deutschland. Diese erfolgt zum einen durch Pressearbeit, aber auch durch themenbezogene Informationen im Internet. Die DVD ist inzwischen als die kritische Datenschutzorganisation in der öffentlichen Wahrnehmung etabliert.

Das Organ der DVD, die DANA, findet in der Datenschutzdiskussion wegen ihrer Berichterstattung, aber vor allem auch wegen ihrer pointierten Positionen große Beachtung. Die DANA zielt darauf ab, die aktuellen Entwicklungen zu dokumentieren, zu kommentieren und zu diskutieren. Jedes Heft hat einen eigenen Schwerpunkt, wobei die gesamte Palette des privaten und des öffentlichen Bereichs abgedeckt wird. Behandelt wird alles, was relevant ist, von der Gen- und Biotechnik über moderne Verfahren der Videoüberwachung, von Chipkarten bis hin zu Expertensystemen und Mustererkennungsverfahren. Sie beschäftigt sich mit Datenschutz in der Schule, im Betrieb, bei der Polizei, bei der Forschung …

Das Internet ist ebenso präsent wie die konventionelle Führung von Arztakten. Angesichts der überbordenden Fülle von Datenschutzliteratur nahm der Verein in der jüngeren Zeit davon Abstand, eigene Buchpublikationen herauszubringen.

Auf Anfrage stehen ExpertInnen aus den Bereichen Recht, Informationstechnik, betrieblicher Datenschutz und Wissenschaft als ReferentInnen für Veranstaltungen zur Verfügung. Daneben gibt es, teilweise gemeinsam mit anderen Organisatoren, ein kleines eigenständiges Seminarangebot. In den 70er und 80er Jahren wurden regelmäßig, in den 90er Jahren unregelmäßig größere Jahrestagungen durchgeführt.

Eine wichtige Aufgabe sieht die DVD in politischer Lobbyarbeit. Durch Gutachten zu politischen Initiativen von Fraktionen und Regierungen ist die DVD immer wieder bei Sachverständigenanhörungen des Bundestages und der Länderparlamente präsent. Aber auch für sonstige Einrichtungen werden bei Bedarf Stellungnahmen und Gutachten angefertigt. Ende der 80er Jahre war die DVD zudem an einem großen Forschungsprojekt der Technischen Universität Berlin beteiligt.

Koalitionspartner

Es gibt eine Vielzahl von Organisationen, mit denen die DVD in Sachen Datenschutz zusammen arbeitet.

Während in den Frühzeiten eine gute Zusammenarbeit zu den Gewerkschaften erfolgte, erlahmte deren Interesse am Datenschutz, was seinen Ausdruck auch darin fand, dass der Deutsche Gewerkschaftsbund Anfang der 90er Jahre seine Mitgliedschaft in der DVD kündigte. Dessen ungeachtet bestehen weiterhin in Einzelfällen Kooperationsansätze.

Zu den sonstigen Datenschutzorganisationen in Deutschland hat die DVD ein unverkrampft freundliches Verhältnis. Über den Austausch von Referenten und Materialien geht aber die Kooperation nicht hinaus. Dies liegt daran, dass sich die Gesellschaft für Datenschutz und Datensicherheit (GDD) als Organisation der Datenverarbeiter und deren Datenschutzbeauftragten versteht und daher teilweise völlig andere Interessen verfolgt. Für den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. stehen berufständische Interessen im Vordergrund. Damit ist die DVD der einzige Datenschutzverband mit bürgerrechtlicher Schwerpunktsetzung.

Die Kooperation mit sonstigen Bürgerrechtsorganisationen ist dementsprechend gut. Dies gilt etwa für die Humanistische Union, das Institut für Bürgerrechte & öffentliche Sicherheit (Bürgerrechte & Polizei/CILIP) oder die Kritischen PolizistInnen.

Eine enge Verbindung besteht zu kritischen Informatikverbänden. Hier sind vorrangig zu nennen das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und das Institut für Informationsökologie (IKÖ).

Zu den politischen Parteien besteht ein eher distanziertes Verhältnis. Zwar zeigt sich, dass insbesondere von der SPD und von Bündnis 90/Die Grünen teilweise gleichgelagerte politische Ziele verfolgt werden. Die kritische Distanz erweist sich insbesondere dann als notwendig, wenn diese Parteien an Regierungen beteiligt sind. Grundsätzlich steht die DVD aber auch zur Beratung der anderen Parteien zur Verfügung, was in der Praxis auch ab und zu in Anspruch genommen wird.

Eine kritische Distanz drängt sich ebenso in Bezug auf die Datenschutzbehörden auf. Zum einen verfolgen diese wie die DVD das gleiche Grundrechtsanliegen. Zum anderen aber gibt es gerade dort viel zu kritisieren. Mangelndes Engagement, Zauderhaftigkeit und Unbestimmtheit, bürokratische Auswüchse, Verflechtungen mit Behörden und Politik sind immer wieder Anlass, die Datenschutzbehörden zu tadeln. Hinzu kommt, dass deren materielle und personelle Ressourcen oft derart dürftig sind, dass ein wirksamer Schutz des Rechts auf informationelle Selbstbestimmung in Frage steht.

Es ist die gesellschaftliche Funktion der DVD, hier die Finger in die vielen Wunden zu legen. Wer sonst würde den Mund aufmachen, wenn über Jahre hinweg in Thüringen die gesetzlich vorgesehene Stelle des Datenschutzbeauftragten einfach nicht eingerichtet wird? Wer sonst sollte die Beauftragten für den Datenschutz immer wieder ermahnen, sich nicht zu sehr in die Regierungspolitik einbinden zu lassen? Es bestehen viele informelle und personelle Kontakte zum behördlichen Datenschutz; ab und zu werden gar Veranstaltungen gemeinsam durchgeführt.

Von Anfang an warf die DVD ein Auge auf die Datenschutzentwicklung in den anderen Ländern Europas und in der Welt. Kooperationen erfolgten mit der österreichischen ARGE Daten, dem britischen Statewatch und in größerem Umfang mit der – inzwischen nicht mehr bestehenden – niederländischen Stichting Waakzaamheid Persoonsregistratie.

Bei der internationalen Kooperati-

Kostenlose Hilfe für „datengestörte" Bürger

In 15 Städten kümmert sich Verein um Datenschutz

Bonn (dpa) — Von der Öffentlichkeit weitgehend unbemerkt wurde im vergangenen Jahr in Bonn die „Deutsche Vereinigung für Datenschutz DVD" gegründet, die sich in erster Linie dem Schutz der Bürger vor mißbräuchlicher Verarbeitung ihrer Daten widmet. Inzwischen hat sich die DVD gemausert und im Bundesgebiet — so in Hamburg, Berlin, Köln, Stuttgart, Marburg, Wiesbaden, Freiburg, München, Hannover und Saarbrücken — insgesamt 15 Außenstellen eingerichtet.

„Datengestörte" Bürger — nicht nur DVD-Mitglieder — können sich dort kostenlos über Probleme der Elektronischen Datenverarbeitung (EDV) beraten lassen, sofern nicht ausgefeilte, dann allerdings auch kostenpflichtige, Gutachten gewünscht werden. Sorge bereitet den ausschließlich ehrenamtlich tätigen DVD-Oberen noch, daß „vielen Leuten gleichgültig ist, was mit ihren Daten geschieht".

Dennoch ist man überzeugt, zumindest auf längere Sicht, eine Marktlücke entdeckt zu haben. Schließlich stehe im Vordergrund nicht die Frage, wie die speichernden Stellen dem Datenschutzgesetz genügten, sondern wie sich die Bürger vor Datenmißbrauch schützen könnten. „Die Problematik der Mißbrauchverhinderung bürgernah verständlich zu machen", ist denn auch eine der Hauptaufgaben der Vereinigung.

Holsteinischer Courier vom 21.09.1978

on erweisen sich aber die begrenzten Möglichkeiten einer auf Ehrenamtlichkeit basierenden Arbeit. So wäre es zwar dringend notwendig, enger mit der staatenübergreifenden Organisation Privacy International zusammenzuarbeiten, die z.B. in einzelnen Ländern einen Big Brother Award verliehen hat, wäre es gut, sich innerhalb der europäischen Union stärker auszutauschen und in länderübergreifende Datenverarbeitungsprojekte (z.B. Europol, Schengen, Enfopol, Echelon, Eurodac) einzumischen. Doch ist das mit den derzeitigen begrenzten Mitteln nicht möglich. So bleibt es zumeist bei der Beobachtung der internationalen Entwicklung und deren Dokumentation in der DANA.

Spezielle Themen

In besonderem Maße war die DVD während der Anti-Volkszählungskampagnen 1983 und dann auch 1987 gefordert. Beides waren Anlässe, um das Thema Datenschutz populär in der Öffentlichkeit zu tragen. Damit in engem Zusammenhang standen die Kontroversen um die Einführung des maschinenlesbaren Personalausweises und um die Verabschiedung der sog. Sicherheitsgesetze. Es war nicht möglich, die vielfältigen regionalen Anti-Volkszählungs-, Mikrozensus-, Anti-Überwachungs- und Anti-Kabel-Initiativen in die DVD-Arbeit zu integrieren. Diese nutzten vielmehr die Fachkompetenz der DVD als eine Art Dienstleister.

Ähnliches gilt für die Unterstützung von Kriegsdienstverweigerern oder für die Unterstützung von Patienteninitiativen bei der Einführung der maschinenlesbaren Krankenversichertenkarte durch die DVD.

Die Datenverarbeitung bei der Polizei stand immer wieder auf dem Prüfstand des Verbandes.

Die langwierigen Novellierungsbemühungen des BDSG, die 1990 endlich ein Ergebnis zeigten, wurden kritisch begleitet. Schon damals wurden von der DVD die technische Antiquiertheit der damals noch neuen Regelungen moniert.

Die DVD war die Organisation, die schon Ende der 80er Jahre immer wieder die Problematik der Videoüberwachung im öffentlichen Raum thematisierte.

Ein weiteres Thema war die Verdatung der AusländerInnen, insbesondere mit Hilfe des Ausländerzentralregisters. Im Rahmen der Novellierung des Ausländergesetzes 1990 wurde der Widerstand gegen die darin vorgesehene Denunzierungspflicht gegenüber den Ausländerbehörden unterstützt. Als 1995 bekannt wurde, dass eine weitgehende Kontrolle von Flüchtlingen durch eine AsylCard geplant sei, war es wieder die DVD, die dieses weitere Kontrollprojekt zu skandalisieren versuchte.

Der Datenschutz in Europa (Europa ohne Grenzen – grenzenlose Kontrolle) war schon früh im Jahr 1989 Gegenstand einer internationalen Tagung. Diese Diskussion fand ihre natürliche Fortsetzung 1994/95 mit der Problematisierung der Datenverarbeitung bei Europol und deren Vorgängerinstitutionen. Obwohl man sich nach der Wende auch ostdeutschen Themen (z.B. Stasi, Einführung von Datenschutzbehörden und -gesetzen) annahm, war es für den Verband bis heute nicht möglich, in den neuen Ländern Fuß zu fassen. Beim Datenschutz handelt es sich – ähnlich wie beim Umweltschutz – leider immer noch um ein westdeutsches Thema.

In den 90er Jahren gewannen technikbezogene Fragen des Datenschutzes eine immer größere Bedeutung. Telekommunikation, Internet, Expertensysteme, Mobilfunk, Chipkarten als technische Rahmenbedingungen machten eine stärker informatikbezogene Diskussion erforderlich, in der z.B. Kryptologie, Pseudonymisierungsmethoden sowie sonstige Privacy Enhancing Technologies eine zentrale Rolle spielen. Kampagnenorientierte Aktivitäten wurden zur datenschutzwidrigen Vermarktung von Telefonbuch-Daten auf CD-ROM (1995) und zur bundesweiten Gebäudedatenbank CityServer (1999) entwickelt.

An anderen öffentlichen Diskussionen, etwa über den sog. Großen Lauschangriff und der damit verbundenen Änderung des Art. 13 Grundgesetz (1998) nahm die DVD eher begleitend als initiierend teil. Datenschutzkampagnen anderer Organisationen, wie z.B. die der HU zur BahnCard und der Koppelung von Bahnpreisvergünstigungen mit Kreditgeschäften und einer aufgezwungenen Datenverarbeitung in den USA, wurden unterstützt.

Als die derzeit wohl wichtigste Aufgabe sieht es die DVD an, sich an der Debatte um die Anpassung des BDSG

an die Europäische Datenschutzrichtlinie und um dessen Modernisierung zu beteiligen. Zu diesem Zweck wurde unter Leitung der DVD ein Arbeitskreis ins Leben gerufen, der einen kompletten neuen BDSG-Entwurf vorlegte. Dieser wurde von der Fraktion Bündnis 90/Die Grünen 1998 in den Bundestag eingebracht. Obwohl dieser Entwurf von allen Seiten, nicht nur von der Datenschutzpraxis, sondern auch aus der Wirtschaft und der Wissenschaft, gelobt wurde, fand er nach dem Wechsel zur rot-grünen Bundesregierung im Bundesministerium des Innern (BMI) keinen Gefallen und wurde nicht berücksichtigt. Vielmehr wagte es das BMI, zunächst einen wortidentischen Entwurf aus schwarz-gelben Zeiten vorzulegen. Dessen ungeachtet blieb der grüne Entwurf bis heute eine wichtige Diskussionsgrundlage für die Novellierung der Landesdatenschutzgesetze und die Vorlage für einige Verbesserungen im BDSG-Entwurf des BMI.

Erfolge oder vergebliche Mühe?

Rekapitulieren wir heute die über 20jährige Arbeit der DVD, so lässt sich diese schon als Erfolgsgeschichte darstellen. Insbesondere zur Förderung des Bewusstmachungsprozesses bei einer Vielzahl von Datenschutzfragen hat die DVD als Katalysator gewirkt. Dabei hatte sie im Konzert der sonstigen Beteiligten eine eigene, eigenwillige Stimme.

Sicherlich sind die Datenschutzbeauftragten als staatliche Stellen mit einem funktionsfähigen professionellen Apparat in erheblich größerem Umfang öffentlich präsent als eine kleine Bürgerrechtsorganisation. Es ist aber schon bezeichnend, dass sich die Medien gerne an die DVD wenden, wenn ihnen die Stellungnahmen der offiziellen Datenschützer zu zahm und defensiv erscheinen.

In einigen Bereichen ist es der DVD gelungen, Datenschutzthemen von sich aus in die Öffentlichkeit zu bringen, z.B. die Ausländerverdatung, das Datensammeln bei Europol oder die Herausgabe von Telefonbuch-CD-ROM. Hier, wie bei sämtlichen sonstigen Fragestellungen, blieb der DVD aber nur die Reaktion auf eine laufende politische oder technische Entwicklung. Sie hat es nie geschafft, eigenständig gestaltend einzugreifen; es blieb regelmäßig beim Problematisieren von bestehenden gefährlichen Projekten. Lediglich in der aktuellen Diskussion um die BDSG-Novellierung war es möglich, kurzfristig die Diskussion selbst zu gestalten.

Die Früchte der DVD-Arbeit sind nur schwer auszumachen. So ist es kaum möglich festzustellen, welchen Beitrag die DVD auf die Anti-Volkszählungsbewegung und welchen diese auf das Volkszählungsurteil des Bundesverfassungsgerichtes hatte. Die DVD ist als Graswurzelinitiative weit von den letztendlich zu erntenden Früchten der Datenschutzpolitik entfernt. Diese Rolle wird durch die schon dargestellte Dienstleistungsfunktion einer fachbezogenen Querschnitts-Initiative verschärft.

Die BürgerrechtlerInnen mit juristischem und informationstechnischem Sachverstand sind als DatenschützerInnen zwar nahe an den Problemen, aber zumeist nur indirekt betroffen. Für die Thematisierung ihres Anliegens sind sie auf die Betroffenheit anderer angewiesen. Diese nehmen die Datenschutzexpertise gerne an.

Ausländer- und Flüchtlingsinitiativen sind natürlich dankbar, kompetent über die informationstechnische und rechtliche Kontrolle von Nichtdeutschen aufgeklärt zu werden. Hauseigentümer nehmen bereitwillig die datenschützerische Hilfe an, wenn ihre Gebäude bundesweit digitalisiert werden. Berufliche Geheimnisträger und JournalistInnen sind natürlich froh über den Hinweis von Datenschützern, dass durch Wohnraum- oder Telekommunikationsüberwachung die Vertraulichkeit ihrer Arbeit in Frage gestellt wird. Die Skandalisierung des Themas bleibt aber zumeist den Betroffenen selbst überlassen. Nur selten liegt der Fall so, dass alle oder viele betroffen sind und der Skandal in der (befürchteten) Generalüberwachung liegt – wie bei den vergangenen Volkszählungen.

Perspektiven

Gäbe es die DVD nicht, so müsste man sie erfinden.

Wir leben in einer pluralistischen Gesellschaft, in der Interessen organisiert werden müssen, um sie öffentlich zur Geltung zu bringen. Dass informationelle Selbstbestimmung in einer Informationsgesellschaft für die Wahrung von Demokratie, Rechtsstaatlichkeit und Bürgerrechtsschutz unabdingbar sind, dürfte unbestreitbar sein. Daher bedarf es der Organisation des Datenschutzes. Dies hat auch das Bundesverfassungsgericht erkannt, als es unabhängige Datenschutzbeauftragte als eine Grundbedingung des Grundrechtsschutzes erklärte „wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatisierten Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes".

Dass aber Datenschutzbeauftragte tatsächlich unabhängig sind und bleiben, ist keine Selbstverständlichkeit. Insofern kann und muss die DVD Stachel im Fleisch auch der Datenschutzbeauftragten sein.

Ein kleiner Bürgerrechtsverband ist natürlich mangels Geld, Personal und verfügbarer Technik nicht in der Lage, die technologische Entwicklung in eine datenschutzfreundliche Richtung zu wenden. Dies schaffen selbst die meistens besser ausgestatteten Datenschutzbeauftragten nicht. Schon eher ist es möglich, bzgl. der rechtlichen und sozialen Rahmenbedingungen mitzugestalten. Um so wichtiger ist die Schiedsrichterrolle der Datenschutzbeauftragten bei der Informatisierung unseres Alltags. Und um so wichtiger sind Stellen, die diesen Prozess kritisch begleiten. Dies gilt für so unterschiedliche Themen wie die staatliche Freigabe von Kryptografie, die Gewährleistung unbeobachtbarer, anonymer elektronischer Kommunikation, die Möglichkeit von Selbstschutzmitteln der Internet-Nutzenden, die (informationstechnisch plötzlich mögliche) Schaffung von Verwaltungstransparenz durch Informationsfreiheit, die Kontrolle großer wirtschaftlicher Datenbanken mit persönlichen Kommunikations-, Konsum- und Liquiditätsprofilen.

Die DVD kann nur eine dieser kritischen Stellen sein. Andere müssen sich über diese ihre gesellschaftliche Aufgabe erst klar werden. Das gilt an vorderster Stelle für Gewerkschaften und Verbraucherverbände. Das gilt aber auch für Selbsthilfeorganisationen und Betroffenenverbände. Das gilt letztend-



DVD-Vorstandsmitglieder im Jahre 1979 (v.l.n.r):
Dr. Gerhard von Keußler (Vors.), Dr. Klaus Hümmerich, Gert Hausmann, Peter Gola, Barbara Schmidt-Belz

lich auch für die politischen Parteien, bei denen aber der Bewusstwerdungsprozess noch am wenigsten festzustellen ist. Die DVD erfüllt eine wichtige gesellschaftliche Funktion, wenn sie gegenüber diesen teilweise mächtigen Interessenverbänden eine Katalysatoren- bzw. eine Moderatorenrolle im Interesse des Grundrechtsschutzes einnimmt.

Sicherlich hat sich der Datenschutz gesellschaftlich etabliert. Zugleich erfolgte eine massive Kommerzialisierung. Große Wirtschaftsunternehmen lassen sich eine interne Datenschutzorganisation etwas kosten, um nicht durch das Bekanntwerden von Verstößen und Skandalen in Verruf zu kommen und Wettbewerbsschäden zu erleiden. Bei vielen Produkten, mit denen die Informatisierung unseres Alltags vorangetrieben werden, ist Datenschutz zu einem Wettbewerbsfaktor geworden, z.B. die Verschlüsselung von Funktelefonen, die technische Abhörsicherung von Anrufbeantwortern, die Wahlmöglichkeit anonymer Nutzungen bei Online-Diensten oder die Nutzung anonymer Prepaid-Chipkarten oder generell hinsichtlich des Angebots von datenschutzfreundlichen Techniken.

Auch an anderen Stellen hat sich ein Datenschutzmarkt entwickelt, z.B. bzgl. Seminaren oder Datenschutzliteratur. So richtig es ist, dass Datenschutz – in einem noch unzulänglichen Umfang – marktfähig geworden ist, so richtig ist es auch, dass der Datenschutz dem Markt nicht überlassen werden darf. Die BürgerIn kann eben ihre Privatheit nicht immer zu Markte tragen. Im Interesse der Wahrung des Persönlichkeitsschutzes sollte sie dies auch nicht müssen.

Es gibt viele Bereiche, in denen Datenschutz nicht marktgängig sein kann, etwa beim Schutz von Minderheiten oder von technisch weniger Versierten oder bei indirekten Konsumbeziehungen. Es ist leider so, dass datenschutzgerechte Rahmenbedingungen nicht zwischen den Vertragspartnern ausgehandelt werden können, wenn technische Standards, branchenweite Absprachen oder gar verarbeitungsfördernde Gesetze dem entgegenstehen. Hier sind vertrauenswürdige Dritte, z.B. informationstechnisch orientierte Bürgerrechtsorgansiationen wie die DVD, als politische Lobby gefordert. Erst recht gilt dies natürlich weiterhin für den hoheitlichen Sektor, wo sich die StaatsbürgerIn ihrer Erfassung nur unter Verletzung rechtlicher Normen entziehen kann.

Wir wollen nicht vermessen sein. Aber sollte das oben Dargelegte zutreffen, so muss man sich auf politischer Ebene Gedanken machen, wie die gesellschaftliche Aufgabe von Bürgerrechtsverbänden noch besser erfüllt werden kann. Schon zu Beginn der 90er Jahre wurde von der DVD vorgeschlagen, grundrechtsorientierten Organisationen in der Informationsgesellschaft ähnliche Rechte einzuräumen wie sie Verbraucherverbänden in derselben Konsumgesellschaft und Umweltverbänden in ebenderselben Risikogesellschaft gewährt werden. Gemeint sind Beteiligungsrechte im Rahmen von informationstechnischen Entscheidungsprozessen und Klagerechte zur Geltendmachung von bürgerrechtlichen Risiken, die nur mit Mühe individualisiert werden können.

Die Verdatung des Menschen – z.B. durch das Rechenzentrum eines rie-

sigen Fnanzdienstleistungskonzerns, durch Adress- und Bonitätsauskunfteien, durch Pressedatenbanken, durch frei verkäufliche CD-ROM oder durch eine online abrufbare Gebäudedatenbank, aber auch durch ein neues polizeiliches Data-Warehouse à la INPOL-neu oder durch flächendeckende Videoüberwachung – hat für jeden einzelnen zwar eine beachtenswerte Auswirkung. Für die gesamte Gesellschaft sind solchen Formen der Informationsverarbeitung aber von gewaltiger Grundrechtsrelevanz. Unabhängigen Verbänden müsste es ermöglicht werden, diese Interessen nicht nur politisch, sondern auch rechtlich verbindlich geltend zu machen.

Zudem sollte darüber nachgedacht werden, wie Bürgerrechtsorganisationen in der Informationsgesellschaft eine von Mitgliedsbeiträgen unabhängige Absicherung ermöglicht werden kann.

Privatheit und Persönlichkeitsschutz ist eben nicht mehr ein Privileg gehobener Gesellschaftsschichten, sondern eine Existenzbedingung einer demokratischen und rechtsstaatlichen Informationsgesellschaft.

Heinz Alenfelder

40 Jahre im Verein – Urgestein oder lebendes Inventar?

Ein recht persönlicher Rückblick auf die ersten 20 DVD-Jahre.

Kaum hatte ich mein Studium aufgenommen (nach heutigen Maßstäben hätte es fast schon vollendet sein sollen), trat die Deutschen Vereinigung für Datenschutz (DVD) in mein Leben. Als interessierter Informatik-Student war ich Teilnehmer der Jahrestagung 1979 „Gefährdet die Informationstechnologie unsere Freiheit?“. Und wie es bei der DVD damals üblich war, wurde ich umgehend für den Vorstand angeworben. Dem folgte bald die „Beförderung“ zum Kassenwart des Vereins. Vielleicht war das meiner Fachrichtung zu danken, denn gegründet wurde die DVD hauptsächlich von Juristen im „Dunstkreis“ der GMD (Gesellschaft für Mathematik und Datenverarbeitung) in Schloss Birlinghoven bei Bonn. Den Überblick über die Finanzen habe ich bis heute als Kassenprüfer behalten.

Halt. Stop. Interessiert das hier? Weitere Details sollte ich den werten Leserinnen und Lesern ersparen, müsste ich doch allzu tief in die Absurditätenkiste des deutschen Vereinswesens greifen. Obwohl, eine Episode soll‘s noch sein: Wegen Verstoßes gegen Einladungsfristen in der Satzung wurde der zuvor gewählte Vorstand mit mir und weiteren vier Mitgliedern vom Vereinsregistergericht entlassen und ein einziges dieser Vorstandsmitglieder zum alleinigen Not-Vorstand bestimmt – dies war dann wieder ich. Nach satzungsgerechter Einladung durfte schließlich – durch die neue Mitgliederversammlung zum zweiten Mal gewählt – der komplette Vorstand sein Amt wieder wie zuvor bekleiden. Das war meine erste Begegnung mit bürokratisch kontrollierter Demokratie!

Das Auf und Ab der DVD ist – im Gegensatz zur landläufigen Vorstellung von Vereinsleben – allerdings nicht geprägt von Rangeleien um Ämter und Pöstchen. Vielmehr stand im Vordergrund immer die inhaltliche Arbeit, deren schier unüberschaubar großer Umfang und die immerwährende Suche nach (halbwegs aktiven) Mitgliedern. Blickte der Vorstand in den ersten 10 Jahren noch stolz auf eine Liste mit 12 Außenstellen in der alten Bundesrepublik, so findet die Meta-Suchmaschine metager.de heute mehrere hundert Treffer zum offiziellen Vereinsnamen. Als Folge des Spagats, der durch den Anspruch, sowohl Bürgerrechtsverein als auch Fachorganisation zu sein, entsteht, hat sich die Mitgliederzahl der DVD in all den Jahren kaum verändert. Konstant blieb auch der Etat, der überwiegend aus Mitgliedsbeiträgen finanziert wurde und wird.

Im Vordergrund der Vereinsarbeit stand, neben der Erstellung von fachlich hochqualifizierten Stellungnahmen, der Beteiligung an diversen parlamentarischen Anhörungen und der Durchführung von bundesweiten Fachtagungen, die Herausgabe der Datenschutz-Nachrichten (DANA). Aufgrund einer recht dünnen Personaldecke konnten aber viele spannende Projekte nicht weiter verfolgt werden. Dennoch: auch wenn der Standardsatz auf Mitgliederversammlungen „Man müsste mal ...“ lautete und diesem seitens der Ideengeber oft keine weiteren Aktionen folgten, wurden aus meiner Sicht vor allem durch die Publikationen sehr viele Gedanken, Ideen und Anregungen fixiert und verbreitet.

Ein Manko des bundesweiten Vereins war die Tatsache, dass aktive Mitglieder zum Austausch und zu Veranstaltungen wie Vorstandssitzungen und Versammlungen weite Reisen in Kauf nehmen mussten. In den ersten 20 Jahren war die Konzentration im Köln-Bonner-Raum Grundvoraussetzung für das funktionierende Vereinsleben. Dank moderner Kommunikationstechniken ist die Notwendigkeit langer Reisen heute kleiner geworden. Weiterhin ist aber die Geschäftsstelle, die nach vielen Umzügen einen sehr guten Heimathafen in den Räumen des Wissenschaftsladens Bonn gefunden hat, Dreh- und Angelpunkt der DVD. Hier laufen die Fäden der Arbeit zusammen.

Was sind nun die Höhepunkte der fast vierzigjährigen Mitgliedschaft im Verein? Sicherlich hat jedes Mitglied andere Höhepunkte erlebt. Für mich persönlich war es die Zeit der Vorstandsmitglied-

schaft und als verantwortlicher DANA-Redakteur von 1986 bis 1996. Die Datenschutz-Nachrichten (DANA) avancierten vom anfangs rein maschinengeschriebenen, später aufwändiger gestalteten Textwüstenmonster zu der Fachpublikation, die sie heute sind. Sie werden nicht nur in Fachkreisen gelesen, die DANA ist anerkannt, niveauvoll und wird häufig zitiert. Auch zeigt die Internet-Recherche, dass die Zeitschrift in den meisten Hochschulbibliotheken ausgeliehen werden kann.

Die DVD präsentiert sich übrigens seit 1998 im WWW mit einer Webseite, damals unter der Adresse www.aktiv.org/DVD, fünf Jahre später unter der heute gültigen Adresse www.datenschutzverein.de. Die Webseite ist seitdem Kommunikationsplattform der DVD. Wurden zur Zeiten der Bundeshauptstadt Bonn Presseerklärungen im Pressehaus an die Redaktionen verteilt, sorgen heute E-Mail-Verteiler und Twitter & Co. für die Verbreitung von Veröffentlichungen. Lediglich die DANA-Ausgaben werden im ersten Jahr nach Erscheinen rein in Papierform angeboten und sind danach erst als PDF-Dokument von der Webseite abrufbar.

Abschließend bleibt das Gefühl, in diesem Verein mit Gleichgesinnten „an einem Strang“ zu ziehen und sich auf die jeweils aktiven Mitglieder verlassen zu können. Hier ist zweifelsohne bundesweit die höchste Konzentration an Datenschutz-Sachverstand zu finden und hier gibt es auch die größte Kontinuität. In der Hoffnung, dass dieser Rückblick nicht mein letzter Beitrag zum Wohle des Vereins war, verbleibe ich mit besten Grüßen an alle Leserinnen und Leser.

Frank Spaeing

Die Entwicklung der DVD in den letzten zehn Jahren

Beim Lesen der verschiedenen Grußnoten und vor allen Dingen beim Lesen der Artikel über die Geschichte der Deutschen Vereinigung für Datenschutz e.V. (DVD) fällt mir vor allem Eines auf: Ich bin das (verzeihen Sie den englischen Ausdruck) „New kid on the block“. Und das in mehr als einer Hinsicht.

Zum einen habe ich mich, als die DVD gegründet wurde, regelmäßig auf meine Grundschulbesuche gefreut, hatte also noch nicht wirklich Interesse am Datenschutz und habe auch die meisten der wesentlichen frühen Entwicklungen (wie zum Beispiel das Volkszählungsurteil von 1983), die den Datenschutz zu dem gemacht haben, was er heute ist, nicht bewusst wahrgenommen.

Meine persönlichen ersten Berührungspunkte mit diesem Thema ergaben sich interessanter Weise bei einer „Public Domain“-Veranstaltung des damaligen FoeBud e.V. in Bielefeld, im Bunker Ulmenwall. Bei einem dieser Treffen hatte ich mich angeregt mit einem der Anwesenden unterhalten und hatte, da ich den Kontakt für mich als hilfreich empfand (wir haben herrlich über die damals aktuelle PC-Technik diskutiert), meinen Gesprächspartner gefragt, ob ich seine Telefonnummer haben dürfe. Ich wollte sie mir auf meiner Liste von Telefonnummern der für mich wichtigen Personen aufschreiben (damals war das ein vielfach gefaltetes DIN-A4-Blatt, beschrieben in engen handschriftlichen Notizen). Er fragte mich, wozu genau ich denn diese Daten sammeln würde, er sei sehr bewusst im Umgang mit seinen Daten (ich bekam aber glaube ich trotzdem nach weiteren Diskussionen seinen Namen sowie die Telefonnummer). Das waren damals für mich neue und spannende Gedanken, mit denen er sich beschäftigte. Mein Studium führte mich dann bald nach Berlin und damit endete (bevor sie richtig beginnen konnte, ich war immer nur interessierter Gast) meine Karriere beim FoeBud.

Zum anderen hat mich mein Lebenslauf nicht auf dem direkten Weg zum Datenschutz gebracht. Es hat mich dieses Thema zwar seit diesen ersten Berührungen nicht wieder losgelassen, aber intensiven Einfluss auf mein Leben hatte der Datenschutz erst wieder nach meiner Entscheidung im Jahr 2006, meine selbstständige Tätigkeit auf den Datenschutz hin auszurichten. Und somit kam ich dann zuerst mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., dann mit der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) und irgendwann im Spätherbst 2011 auch mit der DVD in Berührung, deren Mitglied ich zum Jahresende schnell noch wurde. Im Oktober 2013 wurde ich auf der Mitgliederversammlung dann als Beisitzer in den Vorstand gewählt und auch darum bin ich das „New Kid on the Block“, denn vieles von dem, was die DVD in den ersten Jahren bewegt und erreicht hat, habe ich meist erst nachträglich erfahren.

Ich finde dieses Heft auch deswegen so spannend, da es mir, neben dem Text „Meilensteine“ auf der DVD-Webseite[1], den Sie als ersten Artikel abgedruckt in diesem Heft wahrscheinlich bereits gelesen haben, doch einige andere (durchaus persönliche) Rückblicke auf 40 Jahre DVD bietet, die mir ein besseres Verständnis für die DVD, der ich als Vorsitzender ja mittlerweile vorstehe, ermöglichen.

Ich möchte diesen Artikel nun nutzen, Ihnen die Entwicklung der DVD in den letzten zehn Jahren, die ich (zumeist) bewusst wahrgenommen und auch begleitet habe, darstellen:

Leider habe ich das Highlight des Jahres 2007, den Datenschutztag 2007 in Bielefeld mit vielen Datenschutz-

prominenten, nicht wahr- und folgerichtig auch nicht daran teilgenommen, ich wäre gerne dabei gewesen. Am 11.10.2007 fand tagsüber in der Ravensberger Spinnerei in Bielefeld der Datenschutztag zum 30. Jubiläum der DVD statt. In seinem auf Einladung der DVD gehaltenen Festvortrag richtete sich der Bundesminister a.D. Dr. Dr. h.c. Burkhard Hirsch an die erschienenen Gäste. Die Festveranstaltung ging nach weiteren Beiträgen von Prof. Dr. Wolfgang Däubler (Universität Bremen), padeluun (FoeBuD e.V.), Dr. Johann Bizer (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) und weiteren namhaften Datenschützern über in die Verleihung der BigBrotherAwards 2007, welche von der DVD und FoeBud gemeinsam mit anderen Datenschutz- und Bürgerrechtsvereinen vergeben wurden. Bielefeld war damit am 11. Oktober 2007 zur „Datenschutzhauptstadt Deutschlands" geworden. Das in diesem Zusammenhang dem damaligen Innenminister Wolfgang Schäuble die Ehrenmitgliedschaft für seine Verdienste um das Datenschutzbewusstsein[2] angetragen wurde, passte gut zu diesem Tag.

Interessanterweise hat er meines Wissens nach bis heute nicht auf dieses Angebot reagiert.

Im Jahr 2008 beschäftigte die DVD sich neben vielen anderen Themen[3] (u.a. „Kabinett beschließt ELENA-Gesetzentwurf", „SPD will Grundrecht auf Informationsfreiheit im Internet" (Dieses haben wir ja auch mit dem Urteil des Bundesverfassungsgerichts vom 27.02.2008 bekommen, welches das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" in den Leitsätzen des Urteils etablierte), „Innenministerium plant zentrales Melderegister") auch mit der Aussage des damaligen Innenministers Wolfgang Schäuble „Wir hatten den ´größten Feldherrn aller Zeiten`, den GröFaZ, und jetzt kommt die größte Verfassungsbeschwerde aller Zeiten".

Vielleicht ist es doch nicht so schlecht, dass er kein Ehrenmitglied der DVD geworden ist.

Dass in diesem Jahr auch ein neues BKA-Gesetz verabschiedet wurde, passt da ins Bild.

Das Jahr 2009 war dominiert durch die Novellierung des BDSG, welches im Sommer 2009 beschlossen wurde und in den wesentlichen Teilen am 1. September 2009 in Kraft trat. Hier gab es intransparente Gesetzesänderungen, die vor Beschluss des Gesetzes nicht ausreichend diskutiert werden konnten, es wurde reichlich an der Gesetzesnovelle kritisiert, mal von den Verbraucherschützern, denen vieles nicht weit genug ging, mal von der Wirtschaft, der fast alles viel zu weit ging.

Im Jahr 2010 war (wie schon einige Male vorher) mal wieder über ein Beschäftigtendatenschutzgesetz spekuliert worden. Den damals veröffentlichten Gesetzesentwurf konnte die DVD allerdings nur harsch kritisieren[4].

Komisch, manches scheint sich regelmäßig zu wiederholen.

Im gleiche Jahr fand die gemeinsame Jahrestagung von DVD und dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) am 05./06.11.2010 in Köln statt. Bei der Tagung wurden diverse Themen in Arbeitsgruppen bearbeitet und diskutiert, angefangen mit BewerberInnen-Datenschutz, Forensik, Korruptionsbekämpfung, privacy tools/ Selbstdatenschutz und last but not least Kommunikationsüberwachung im Beschäftigungsverhältnis.

Im Jahr 2011 zog nicht nur die Geschäftsstelle der DVD in die Rheingasse in Bonn, auch wurde anlässlich des Reformvorhabens der Kommission am 19. Oktober 2011 zu einer Informationsveranstaltung ins Europäische Parlament eingeladen. Ende 2011 wurde der erste Entwurf einer neuen Datenschutzgesetzgebung auf europäischer Ebene geleakt[5], die DVD war also mit ihrer Veranstaltung[6] brandaktuell.

Erinnern Sie sich noch an den Sommer 2012? An das Halbfinale Deutschland gegen Italien, an das zu diesem Zeitpunkt beschlossene neue Melderecht[7]? Im Jahr 2012 hatte sich die DVD in Zusammenarbeit mit campact, FoeBud, vzbv und anderen Organisationen dem Protest gegen die Melderechtspläne der Bundesregierung angeschlossen und offenbar die Bundesländer überzeugt, die umstrittenen, weit reichenden Zugänge der Wirtschaft zu unseren Meldedaten neu zu verhandeln. Im gleichen Jahr mobilisierten Verbraucherschützer (auch die DVD) gegen ACTA. Und die DVD veranstaltete am 04.09.2012 im Europäischen Parlament zum zweiten Mal eine Datenschutzveranstaltung für und mit Parlamentarierinnen und Parlamentariern. Die Datenschutz-Grundverordnung (DS-GVO) fing an, ihre Schatten vorauszuwerfen.

Selbst im Jahr 2013 (zumindest noch im Januar[8]) bewegte noch das geplante Beschäftigtendatenschutzgesetz die Gemüter. Im Meldewesen zeichneten sich Besserungen ab[9] und ein neuer Innenminister versuchte ein neues Supergrundrecht zu etablieren[10]. Da hatte unser Appel gemeinsam mit vielen anderen Verbraucherschutzorganisationen[11] wohl nicht viel geholfen. Der Sommer stand komplett im Zeichen der Snowden-Enthüllungen. Zum Ende des Jahres 2013 kommentierten wir dann die Kandidatin der CDU/CSU für das Amt der neuen Bundesbeauftragten für Datenschutz und Informationsfreiheit[12].

Sie merken vielleicht, ich habe die Formulierung geändert, ab der Mitgliederversammlung im Herbst 2013 war ich Mitglied im Vorstand und habe ab dann die meisten Themen aktiv begleitet.

Im Jahr 2014 beschäftigten uns (wieder einmal) die Geheimdienste[13] und es erschien ein neues Schreckgespenst, die PKW-Maut[14]. Bei der Demonstration gegen die Sonderfinanzierung des BND stand ich selbst an einem kalten Novembermorgen mit vorm Reichstag und schwenkte Plakate[15]. Im Anschluss ging ich dann noch mit Kolleginnen und Kollegen in die an dem Tag stattfindende öffentliche Sitzung des NSA-Untersuchungsausschusses[16]. Insgesamt war das ein spannender Tag. Auch wenn die Demonstration in der Nachschau nicht so viel gebracht hat.

Das Jahr 2015 war anfangs auch noch geprägt von der Diskussion über die Geheimdienste, die DVD beteiligte sich an der Verbreitung der von vielen Bürgerrechtsorganisationen getragenen Petition gegen die Erhöhung des BND-Etats[17].

Aber das Hauptthema des Jahres war sicherlich die DS-GVO. Im Frühjahr 2012 war der Entwurf der EU-Kommission veröffentlicht worden, im Oktober 2013 konnte Jan Philipp Albrecht im LIBE-Ausschuss des EU-Parlaments seinen Verhandlungsvorschlag durchbringen und dieser wurde im März 2014 vom EU-Parlament als offizieller Parlamentsentwurf beschlossen. Der EU-Rat hatte erst deutlich später mit seinen Verhandlungen begonnen und einigte sich erst Anfang Juni 2015 auf einen gemeinsamen Entwurf, der deutlich schwächer als der des EU-Parlaments war (auch dieser wurde nicht nur gelobt[18]).

Hier hatten wir nun die Chance, vor Beginn der Trilog-Verhandlungen zur DS-GVO darauf Einfluss zu nehmen. In Zusammenarbeit mit anderen Verbraucherschutzorganisationen konnte die DVD ein DANA-Sonderheft herausgeben, in dem Verbraucherschutzorganisationen, Datenschutzverbände, wichtige Persönlichkeiten des Datenschutzes und nicht zuletzt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihre roten Linien zur DS-GVO aufzeigen konnten, die nicht überschritten werden durften[19]. In sehr kräfteraubender Arbeit schafften wir es (unterstützt durch campact), dass wichtige Entscheider aus dem EU-Parlament und alle Mitglieder des Bundestags dieses Sonderheft passend zu Beginn der Verhandlungen zugestellt bekamen.

Nebenbei war dann auch noch einmal schnell die Geschäftsstelle im Sommer 2015 in neue Räumlichkeiten gezogen, ins WiLa in der Reuterstraße in Bonn. Ein Umzug, den wir nicht bedauert haben.

Dem Thema Datenerfassung und Flüchtlinge widmeten wir die DANA-Ausgabe 2/2015.

Am 06.10.2015 setzte der EuGH ein Ausrufezeichen mit seiner Entscheidung zu Safe Harbor[20]. Und ein anderer „guter alter“ Bekannter war wieder aufgetaucht, die Vorratsdatenspeicherung. Am 16.10.2016 wurde dagegen vorm Bundestag protestiert[21]. Bei der Protestaktion wurden die Unterschriften von über 116.000 Menschen unter einen gemeinsamen Appell gegen Vorratsdatenspeicherung an den SPD-Bundestagsabgeordneten Marco Bülow übergeben. Die Botschaft der Protestaktion: „Nein zum Gläsernen Bürger! Keine Vorratsdaten!”.

Dass wir die für Anfang Oktober 2015 geplante Datenschutztagung „Vernetzt und überwacht“ absagen mussten, war und ist weiterhin schade, denn auch damit bewiesen wir eine Nase für aktuelle Themen, noch heute beschäftigt (nicht nur) uns immer mehr die Frage des Datenschutzes beim Autofahren, besonders auch beim (teil-)autonomen Fahren[22].

Mitte Dezember 2015 einigten sich dann EU-Parlament und EU-Rat im Trilog-Verfahren auf einen gemeinsamen Entwurf der DS-GVO. Womit das Jahr 2015 definitiv eines der spannenderen gewesen ist.

Und auch das Jahr 2016 fing turbulent an, mussten sich doch die EU und die USA auf einen Nachfolger für das obsolet gewordene Safe Harbor einigen. Denn mit dem Urteil des EuGH war eine wichtige Grundlage für die Übermittlung von personenbezogenen Daten aus der EU in die USA weggefallen. Die EU hatte sofort Verhandlungen aufgenommen um die von den europäischen Aufsichtsbehörden für den Datenschutz gewährte Frist bis Februar 2016 nicht zu verschwenden. Allerdings dauerte es dann doch noch recht lange, bis es einen Nachfolger für Safe Harbor gab, den EU-US Privacy Shield – der übrigens nicht wirklich besser ist als Safe Harbor war, aber das ist (nicht) nur meine persönliche Meinung. Diesen Prozess begleiteten wir (wie viele andere Organisationen auch) u.a. durch Pressemitteilungen[23].

Anfang des Jahres 2016 äußerten wir uns erneut zu einer Wahl einer Aufsichtsbehördenleitung[24]. Ich erinnere mich noch lebhaft an viele Diskussionen mit Vertretern verschiedener Aufsichtsbehörden zu diesem und dem nächsten offenen Brief[25] zu Wahlen von AufsichtsbehördenleiterInnen.

Unabhängig davon ging es mit der DS-GVO in den Endspurt. Am 27.04.2016 wurde sie beschlossen und am 04.05.2016 im europäischen Amtsblatt veröffentlicht[26] und trat am 25.05.2016 in Kraft.

Anlass genug für uns, in einem Sonderheft der DANA (2/2016) wieder die Organisationen und wichtigen Persönlichkeiten des Datenschutzes zu ihrer Meinung nach der Einhaltung der im Sonderheft 3/2015 gesetzten roten Linien zu befragen[27].

Und natürlich befassten wir uns ausführlich mit dem zu erwartenden Nachfolger des Bundesdatenschutzgesetzes, welches zum 25.05.2018, zum Gültigwerden der DS-GVO nicht mehr anwendbar sein wird. Schon im August 2016 forderten wir gemeinsam mit Digitalcourage (ehemals FoeBud) ein verbesserndes Datenschutzgesetz, welches die Konkretisierungsmöglichkeiten, die die DS-GVO bietet, zu Gunsten der Betroffenen nutzen sollte[28]. Eigentlich hätten wir es besser wissen können.

Nachdem sich das DANA-Heft 3/2016 mit dem Thema Beschäftigtendatenschutz in neuen Gewändern (im Rahmen der DS-GVO und des zu erwartenden BDSG-Nachfolgers) beschäftigte und nebenbei auch ausführlich über Pokémon GO berichtete[29] (erinnern Sie sich noch an die Horden von auf ihre Handys starrenden Menschen, die sich weltweit lawinenartig durch die Städte und Lande bewegten, immer auf der Jagd nach dem nächsten Pokémon?), wir uns im Herbst 2016 mit dem Videoüberwachungsverbesserungsgesetz[30] und dem neu zu wählenden Landesbeauftragten für den Datenschutz in Mecklenburg-Vorpommern beschäftigten durften (s.o.) wurde dann Ende November 2016 der erste Entwurf des Nachfolgers des BDSG veröffentlicht. Und meine Güte, was war der Entwurf schlecht! Er war so schlecht, dass

wir wieder (wie auch schon beim Videoüberwachungsverbesserungsgesetz) eine (dieses Mal sehr ausführliche) Stellungnahme gemeinsam mit dem Netzwerk Datenschutzexpertise erstellen und veröffentlichen[31] mussten. Das war kein schönes Geschenk zum Jahresende für uns Betroffene. Aber es war ja nur ein erster Entwurf. Wie gesagt, wir hätten es ahnen können.

Im Jahr 2017 ging es mit einer Pressemitteilung zum Vorschlag der EU zur Abschaffung des anonymen Bezahlens im Internet[32] weiter („Kein gläserner Zahlungsverkehr zwecks Terrorismusbekämpfung") und wir hatten noch diverse Entwürfe des BDSG-Nachfolgers (der, man glaubt es kaum wie kreativ, Bundesdatenschutzgesetz (neue Fassung) heißen soll) zu kommentieren[33]. Und dann hatten wir konsterniert zur Kenntnis zu nehmen, dass eine leidlich entschärfte aber trotzdem nicht wirklich gut zu nennende Version beschlossen und verkündet wurde[34]. Ob nun einige Verbraucherschutzorganisationen gegen einzelne Passagen des BDSG-neu vorgehen werden, sobald es gültig geworden ist, oder ob die EU ein Vertragsverletzungsverfahren gegen Deutschland starten wird, weil einzelne Teile des BDSG-neu europarechtswidrig[35] sind, bleibt abzuwarten.

In Abwandlung eines bekannten Satzes kann festgehalten werden: „Ob Du Recht hast oder nicht, sagt Dir das Gericht…".

Was hat uns in diesem Jahr noch bewegt? Nun ja, die EU-Kommission möchte parallel zur DS-GVO auch noch die ePrivacyVO[36] an den Start bringen. Der deutsche Gesetzgeber steht vor der nicht gerade kleinen Aufgabe, alle deutschen Gesetze auf Kompatibilität mit der DS-GVO zu prüfen und diese wo notwendig zu ändern. Schade, dass er dabei regelmäßig versucht, über das Ziel hinauszuschießen[37]. Damit Gesetze gut werden, braucht es transparente Gesetzgebungsverfahren. Aber so eine Erwartung vor einer Bundestagswahl…?

Apropos Bundestagswahlen. Vor der Bundestagswahl 2017 hatten alle Parteien in Parteiprogrammen zum Thema Datenschutz Stellung genommen (oder auch nicht)[38].

Aber Sie wissen ja nun mittlerweile selbst, was bei dieser Bundestagswahl herausgekommen ist. Wir dürfen mehr als gespannt sein, welche Bedeutung Datenschutz für die nächste Bundesregierung haben wird.

Aus Vereinssicht hatten die letzten Jahre durchaus auch ihre turbulenten Seiten:

Ab dem Jahr 2014 ergaben sich im Vorstand der DVD gravierende Veränderungen. Karin Schuler trat Anfang Dezember 2014 von ihrem Amt als Vorsitzende zurück (sie wurde abgelöst durch Sönke Hilbrans, der als erster Stellvertreter auf den Vorsitz nachrückte, neue Stellvertreter wurden Jaqueline Rüdiger als Kassiererin und ich). Sönke Hilbrans hatte eigentlich vor, aus dem Vorstand auszuscheiden (wie auch Karin Schuler auf Grund von überbordender Arbeitslast und dem Wunsch nach Verwirklichung neuer Herausforderungen), stellte seinen Wunsch aber im Sinne einer strukturierten Übergabe und zur Sicherung der Kontinuität der Vorstandsarbeit hintan. Als Vorsitzender blieb er uns bis zur Mitgliederversammlung 2015 erhalten, bis zur Mitgliederversammlung 2016 unterstützte er den Vorstand noch als Beisitzer. Auch Robert Colombara, der die letzten Jahre als Kassierer tätig gewesen war, kündigte in der außerordentlichen Vorstandssitzung am 06.12.2014 seinen baldigen Rücktritt an (mit ähnlichen Argumenten wie Karin Schuler und Sönke Hilbrans). Die Jahre 2014 und 2015 waren also geprägt von personellen Veränderungen des Vorstands, die bis ins Jahr 2016 Auswirkungen hatten und sich auch in diesem Jahr fortsetzten. Jaqueline Rüdiger, die stellvertretende Vorsitzende und Kassiererin schied aus familiären Gründen zu Jahresbeginn aus dem Vorstand aus und wurde von Riko Pieper, der erst im Herbst 2015 als Beisitzer dazu gekommen war, ersetzt.

Auch die Geschäftsstelle hatte in den Jahren zwei personelle Wechsel zu verkraften, der neue Vorstand hatte also schon allein mit interner Organisation genug zu tun. Besonderer Dank gebührt an dieser Stelle Reinhard Linz, der sich der Geschäftsstelle zusammen mit der Kassiererin annahm und alle Prozesse nach den neuen Rahmenbedingungen strukturierte und begleitete (seit seiner Wahl in den Vorstand bei der Mitgliederversammlung im Herbst 2014). Mit Werner Hülsmann im Jahr 2014 und Thilo Weichert im Jahr 2015 konnten wir außerdem auch zwei Alt-Vorstände wieder für die Vorstandsarbeit gewinnen, beide haben sich in den letzten Jahren intensiv für die DVD eingebracht.

Also waren die letzten Jahre nicht nur durch intensive Veränderungen im Datenschutzumfeld geprägt, auch DVD-intern hatten wir einige Baustellen, an denen sich der Vorstand abzuarbeiten hatte. Heißt es nicht angeblich in einem chinesischem Sprichwort „Mögest Du in interessanten Zeiten leben"[39]? Interessante Zeiten fürwahr.

Die Tatsache, dass wir in diesen interessanten Zeiten nicht alleine da stehen, dass es immer wieder Partnerorganisationen und Mitstreiter gegeben hat und auch weiterhin geben wird, mit denen wir gemeinsam Projekte durchführen, ist an der Stelle durchaus beruhigend.

Lassen Sie mich den Rückblick noch mit einer aus DVD-Sicht erfreulichen Tendenz abschließen: Seit dem Jahr 2015 verzeichnen wir regelmäßig steigende Zahlen an Neumitgliedern, allein in diesem Jahr haben wir schon zwanzig neue Mitglieder (fast so viele wie in den Jahren 2015 und 2016 zusammen) gewonnen.

Dies zeigt uns zum einen, dass das Thema Datenschutz so aktuell ist wie selten zuvor (Wie sollte das in interessanten Zeiten auch anders sein?) und dass die DVD zum anderen durchaus viel wahrgenommen wird.

Beides sind keine schlechten Zeichen und eine nach Mitgliederzahlen wachsende DVD sorgt für den dauerhaften Bestand.

Und wenn wir uns die Grußnoten in diesem Heft so anschauen, scheinen wir ja in den letzten 40 Jahren Einiges richtig gemacht zu haben und als relevant und wichtig wahrgenommen zu werden. Beste Voraussetzung also für die nächsten 40 Jahre.

In diesem Sinne wünsche ich uns allen viel Kraft und Durchhaltevermögen um den Datenschutz auch in den nächsten Jahren gegen alle Widrigkeiten voranzubringen.

1 https://www.datenschutzverein.de/vereinsprofil/meilensteine/

2 Zitat aus der damaligen Pressemitteilung zum Datenschutztag 2007: "Mit einer nicht enden wollenden Serie von Vorschlägen zum Abbau des Datenschutzes und zum Aufbau einer umfassenden

staatlichen Überwachung aller Menschen in Deutschland hat er die Öffentlichkeit nachhaltig schockiert und das Bewusstsein dafür geschärft, dass Datenschutz eine notwendige Voraussetzung für die Freiheit in einer modernen Gesellschaft ist."

3 Im Jahresregister 2008 (wie auch in den Jahresregistern der anderen Jahre) kann hervorragend nachvollzogen werden, was damals die Branche bewegte: https://www.datenschutzverein.de/wp-content/uploads/2013/07/DANARegister2008.pdf

4 https://www.datenschutzverein.de/wp-content/uploads/2013/07/2010_PE_Beschaeftigtendatenschutzgesetz.pdf

5 http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

6 wie manches Mal in den letzten Jahren, z.B. auch hier: https://www.datenschutzverein.de/wp-content/uploads/2013/07/2011_EU-RiLi.pdf

7 http://www.spiegel.de/politik/deutschland/meldegesetz-bundestag-stimmte-im-express-tempo-ab-a-843337.html

8 https://www.datenschutzverein.de/wp-content/uploads/2013/03/2013_01_BeschDSG02.pdf

9 https://www.datenschutzverein.de/wp-content/uploads/2013/03/2013_02_MelderechtAbschluss.pdf

10 https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html

11 https://www.datenschutzverein.de/wp-content/uploads/2013/07/2013_05-OB_IM_Friedrich.pdf

12 https://www.datenschutzverein.de/wp-content/uploads/2013/12/2013_12_BfDI.pdf

13 https://www.datenschutzverein.de/wp-content/uploads/2014/06/2014_06-Geheimdienste.pdf

14 https://www.datenschutzverein.de/wp-content/uploads/2014/11/2014_11-Maut.pdf

15 https://www.datenschutzverein.de/wp-content/uploads/2014/11/2014_BNDDemo.pdf

16 https://netzpolitik.org/tag/nsa-untersuchungsausschuss/

17 https://www.datenschutzverein.de/wp-content/uploads/2015/04/2015-01-BND-Etat-Erhoehung-stoppen.pdf

18 siehe zum Beispiel auch hier zum Einfluss von Lobbyisten: http://www.lobbyplag.eu/map

19 https://www.datenschutzverein.de/wp-content/uploads/2016/10/DANA_15_3_Heft.pdf

20 https://www.datenschutzverein.de/wp-content/uploads/2015/10/2015-10-12_DVD-PM_EuGH_zu_Safe_Harbor.pdf

21 https://www.datenschutzverein.de/wp-content/uploads/2015/10/2015-10-16-DVD-PM-Protest_vor_dem_Reichstag_gegen_Vorratsdatenspeicherung.pdf

22 https://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2017_39thIDSK_HongKong_ResolutionOnDataProtectionAutomatedAndConnectedVehicles.html

23 https://www.datenschutzverein.de/wp-content/uploads/2016/02/2016-02-03-DVD_zu_EU-US-Privacy_shield.pdf und https://www.datenschutzverein.de/wp-content/uploads/2016/03/2016-03-01-DVD_schockiert_ueber_EU-US-Privacy_shield.pdf und https://www.datenschutzverein.de/wp-content/uploads/2016/07/2016-07-01-DVD-PE-EU-US-PrivacyShield.pdf und https://www.datenschutzverein.de/wp-content/uploads/2016/07/2016-07-12-DVD-PE-EU-Kommssion_beschliesst_Privacy-Shield.pdf

24 https://www.datenschutzverein.de/wp-content/uploads/2016/01/Offener-Brief-der-DVD-an-die-Berliner-SPD-Fraktion-zur-Nominierung-der-BDI-Kandidatin-vom-16.01.2016.pdf

25 https://www.datenschutzverein.de/wp-content/uploads/2016/11/2016-11-DVD-PE-LfDI-MV.pdf



26 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU&toc=OJ:L:2016:119:TOC

27 https://www.datenschutzverein.de/wp-content/uploads/2016/07/DANA_16_2_Inhalt.pdf

28 https://www.datenschutzverein.de/wp-content/uploads/2016/07/PM-2016-08-01-BDSG-Nachfolgegesetz.pdf

29 https://www.datenschutzverein.de/wp-content/uploads/2016/10/DANA_16_3_Inhalt.pdf

30 https://www.datenschutzverein.de/wp-content/uploads/2016/11/PM_Videoueberwachung_07112016.pdf

31 https://www.datenschutzverein.de/wp-content/uploads/2016/12/Stellungnahme_BDSG-neu_DVD_NW-DSE_20161204_Web.pdf

32 https://www.datenschutzverein.de/wp-content/uploads/2017/01/Kein_glaeserner_Zahlungsverkehr_zwecks_Terrorismusbekaempfung.pdf

33 https://www.datenschutzverein.de/wp-content/uploads/2017/02/2017-02-01-DVD-PE-BDSG-RegE.pdf und https://www.datenschutzverein.de/wp-content/uploads/2017/04/2017-04-26-PE-DVD-BDSG-neu-Bundestag.pdf

34 Dieses war uns als DVD keine Pressemeldung mehr wert, deswegen: https://www.bvdnet.de/bdsg-n-f-dsanpug-eu-im-bundesgesetzblatt-veroeffentlicht/

35 https://netzpolitik.org/2017/grosse-koalition-will-neues-datenschutzgesetz-diese-woche-verabschieden-sachverstaendige-aeussern-massive-kritik/

36 https://www.datenschutzverein.de/wp-content/uploads/2017/05/2017-05-31-PE-DVD-ePrivacyVO.pdf

37 https://www.datenschutzverein.de/wp-content/uploads/2017/05/2017-05-30-DVD-PM-Bundesversorgungsgesetz.pdf

38 https://www.udldigital.de/wahlprogramme-im-vergleich-datenschutz/

39 https://de.wikipedia.org/wiki/M%C3%B6gest_du_in_interessanten_Zeiten_leben



Wenn es die DVD nicht gäbe, man müsste sie erfinden!

Liebe Kolleginnen und Kollegen der DVD,

geht es um Datenschutz, nehmt ihr – während wir uns als Berufsverband oft streng an unsere Satzungsvorgaben gebunden fühlen – kein Blatt vor den Mund. Ihr sprecht Missstände klipp und klar an, kritisiert auch mal mit spitzer Feder – aber stets im Rahmen eines sachlichen Diskurses.

Und selbst wenn manchmal Frust durchblickt: Das ist durchaus erlaubt. Denn oft begegnet uns Datenschützern naive Technikgläubigkeit und unrealistische Erwartungen an die „digital Correctness" von Digital-Unternehmen. Aber der Markt regelt nichts selbst – was man seit Jahren überall sehen kann. Gerade deshalb ist die Botschaft, die von eurer Arbeit ausgeht, nämlich Missstände aufzuzeigen und Lösungen anzubieten, heute wichtiger denn je.

Ich darf wohl sagen, dass diese Arbeit Früchte getragen hat. Natürlich kann sich niemand diese Lorbeeren allein anheften. Gerade in Deutschland und Europa haben viele „Überzeugungstäter" dazu beigetragen, dass wir ein EU-Datenschutzrecht bekommen, welches – bei aller Kritik – das Zeug zu einem echten Exportschlager hat.

Nicht nur die Menschen in Deutschland und Europa sehnen sich nach einem besseren Schutz ihrer Persönlichkeitsrechte. In vielen anderen Ländern, vor allem in den sogenannten Drittstaaten, treten immer wieder auch Verbände für den Schutz der Bürgerinnen und Bürger vor Datenmissbrauch ein. Deshalb lohnt es sich, weiterzukämpfen für einen Datenschutz, der auch zukünftig Wirtschaft und Politik auf die Finger oder gerne auch auf den Mund schaut, damit die digitale Evolution in vertretbaren Bahnen verläuft.

Wir gratulieren euch zum Jubiläum und wünschen weiter viel Energie und Durchblick, damit ihr diese wichtige Aufgabe weiterhin stemmen könnt. Wie in der Vergangenheit werden wir – davon bin ich überzeugt – immer wieder Wege gemeinsam oder zumindest abgestimmt gehen.

Thomas Spaeing
Vorstandsvorsitzender
Berufsverband des Datenschutzbeauftragten Deutschlands (BvD) e.V.

Der BvD: Die Interessenvertretung der Datenschutzbeauftragten

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert die beruflichen Interessen der Datenschutzbeauftragten in Behörden und Betrieben und setzt sich aktiv für die weitere Akzeptanz des Berufsbildes „Datenschutzbeauftragter" ein – als einziger Verband in Deutschland.

digitalcourage

Liebe Gründer.innen, Mitglieder und Aktive der DVD,

Digitalcourage gratuliert euch aufs Herzlichste zum 40. Geburtstag!

Menschen sind schon erstaunt, wenn wir ihnen erzählen, dass wir uns 1987 gegründet haben. Ihr aber seid uns noch um zehn Jahre voraus gewesen. Schon 1977 eine Organisation für Datenschutz als Menschenrecht zu gründen, das zeugt von Weitblick – Chapeau! Und dass die DVD auch weiterhin aktiv ist, das zeugt von Hartnäckigkeit. Also:

Weitblick und Hartnäckigkeit – beides brauchen wir im Kampf für Grundrechte. Egal, welche Themen-Moden, Konzern-PR oder Netz-Filterblasen gerade die Medien beherrschen – es ist wichtig, an den grundsätzlichen Dingen dranzubleiben, ohne die vieles andere auch nichts wert wäre.

Wir schätzen uns glücklich, dass die DVD seit 2000 – also seit Anfang an – bei der Verleihung der BigBrother-Awards mitwirkt – eure Fachkompetenz ist unverzichtbar in der Jury! Ein persönliches „Danke" an Karin Schuler, Sönke Hilbrans, Frans Valenta, Werner Hülsmann und last but not least Thilo Weichert.

Ihr bleibt nicht bei Detailfragen der Durchführung von Datenschutzgesetzen stehen, sondern schaut über den Tellerrand hinweg und engagiert euch für die verdateten Bürgerinnen und Bürger – und das heißt für die Allgemeinheit. Und so haben wir schon bei einigen „Runden Tischen" in Ministerien uns zusammen die Haare gerauft und etliche Aktionen und Kampagnen für besseren Datenschutz gemeinsam gestemmt.

Wir möchten euch ganz herzlich danken. Eure Fachkompetenz und euer Engagement sind wichtig für die ganze Datenschutz-Bewegung! Wir wünschen euch von Herzen viel Erfolg für die nächsten 40 Jahre. Noch mehr wünschen wir uns allen, dass wir gar nicht mehr so lange brauchen, um Europa zum Datenschutz-Paradies zu machen, das globales Vorbild ist.

Jetzt lasst euch feiern!

Allerbeste Grüße
//Rena Tangens, padeluun & das ganze Digitalcourage-Team

Digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Digitalcourage organisierte (damals noch unter dem alten Namen „FoeBuD e.V.,“) die Veranstaltungsreihe „Public Domain“ und baute ab 1989 den Netzknoten BIONIC und die MailBox-Netze Zerberus, CL und Zamir Transnational Network mit auf.

Seit 2000 verleiht Digitalcourage jährlich gemeinsam mit anderen Bürgerrechtsorganisationen die BigBrother-Awards („Die Oscars für Überwachung“, schrieb Le Monde).

Digitalcourage ist gemeinnützig und unabhängig und finanziert sich durch Fördermitgliedschaften und Spenden. 2008 erhielt Digitalcourage die Theodor-Heuss-Medaille für besonderen Einsatz für die Bürgerrechte, 2015 den taz-Panter-Preis für die Helden des Alltags.



Grußwort der Landesbeauftragten für den Datenschutz Niedersachsen und Vorsitzenden der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder 2017, Barbara Thiel

Als diesjährige Vorsitzende der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) gratuliere ich der Deutschen Vereinigung für Datenschutz e.V. (DVD) ganz herzlich zu ihrem 40jährigen Bestehen. Ein solches Jubiläum ist ein guter Anlass, das Vergangene Revue passieren zu lassen, die Gegenwart zu würdigen und zugleich einen Blick in die Zukunft zu richten.

Nahezu zeitgleich mit der DVD hat die DSK, die heute aus der Bundesdatenschutzbeauftragten, den Landesdatenschutzbeauftragten der 16 Bundesländer und dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht besteht, ihre Arbeit aufgenommen. Schon damals erschien eine gewisse Kooperation und Koordination in Fragen des Datenschutzes sinnvoll und notwendig. Waren es ursprünglich nur regelmäßige Treffen, hat sich die DSK inzwischen zu einem Gremium entwickelt, das heute ein nicht zu unterschätzendes Gegengewicht zu den politischen Akteuren auf Bundes- und Landesebene darstellt.

Aktuell stehen die Datenschutzbehörden vor der Aufgabe, sich neu aufzustellen: Egal, ob Safe-Harbour-Urteil, die europäische Datenschutzgrundverordnung oder die Novellierung des Bundesdatenschutzgesetzes – der europäische und damit auch der deutsche Datenschutz befinden sich derzeit im Umbruch. Alle Institutionen, Verbände und Organisationen, die sich für den Datenschutz und das Recht auf informationelle Selbstbestimmung in Deutschland stark machen, stehen, genauso wie die Datenschutzbehörden auf nationaler und europäischer Ebene, vor großen Herausforderungen und sehen sich mit zahlreichen Veränderungsprozessen konfrontiert. Insbesondere in Deutschland, mit seiner föderalen Ordnung, ergeben sich hierbei ganz spezielle Herausforderungen. Es gilt in Europa mit einer Stimme zu sprechen, ohne die bewährte Struktur aufzugeben.

Nach wie vor sind meine Kolleginnen und Kollegen und auch ich fest davon überzeugt, dass ein hohes Datenschutzniveau nicht nur dazu dient, die Einhaltung der Rechte jedes Einzelnen zu garantieren. Denn die Gewährleistung und Einhaltung anspruchsvoller Datenschutzrichtlinien muss letztlich kein Hemmnis für Wirtschaftswachstum darstellen. Vielmehr kann hieraus eine Art Qualitätssiegel kreiert werden, dass deutsche und europäische Unternehmen für Kunden und Verbraucher attraktiv und im internationalen Vergleich wettbewerbsfähig macht. Vor allem im Zusammenhang mit der fortschreitenden Digitalisierung können sich für Unternehmen unter diesem Aspekt ganz neue Möglichkeiten ergeben, wenn sie den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einsetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Mehr denn je sind Datenschützer aber auch darin gefordert, mit der Wirtschaft als vornehmlichen Treiber der Digitalisierung in einen Dialog zu treten und als Ansprechpartner präsent zu sein. Die Herausforderung besteht an dieser Stelle zweifelsohne darin, die Persönlichkeitsrechte von Bürgerinnen und Bürgern zu wahren und den Unternehmen gleichzeitig die Nutzung technologischen Fortschritts zu ermöglichen. Umsetzen lassen sich diese Ziele beispielsweise dann, wenn Unternehmen, Datenschützer aber auch Verbände und Nichtregierungsorganisationen über geeignete Plattformen und Kommunikationskanäle zu einem verstetigten Dialog finden.

Organisationen wie die DVD sind in diesem Zusammenhang vielleicht wichtiger als jemals zuvor. Denn sie sorgen dafür, dass der staatliche Datenschutz nicht die einzige Stimme ist, die für die Wahrung der Bürgerrechte eintritt.

Seit vier Jahrzehnten engagiert sich Ihre Vereinigung für die Belange der Bürgerinnen und Bürger in Sachen des Datenschutzes. Im Laufe dieser Zeit haben Sie nicht nur Expertise in diesem Fachgebiet erlangt und sind selbst zu einer Institution gewachsen, deren Meinung heute nur noch schwer zu überhören ist. Sie haben außerdem bewiesen und beweisen es nach wie vor, wie wichtig aktive und streitbare Akteure unserer Zivilgesellschaft für ein funktionierendes Zusammenleben innerhalb einer Demokratie sind und wie leistungsstark die Zivilgesellschaft sein kann.

Wie gut die Zusammenarbeit zwischen den unabhängigen Datenschutzbehörden

und der DVD funktioniert, lässt sich auch an Publikationen wie den „Roten Linien zur EU-DSGVO“ ablesen. Ihnen ist es zu verdanken, dass noch vor der Einführung der DSGVO ein umfassendes Stimmungsbild profilierter Datenschützer aus dem staatlichen und dem zivilgesellschaftlichen Bereich vorgelegen hat und auf Gefahren und Kritikpunkte im Zusammenhang mit dem neuen EU-Recht aufmerksam gemacht werden konnte.

Dass die DVD diesen Einsatz nun bereits seit 40 Jahren zeigt, ist ein Grund zum Feiern. Vor allem ist es aber ein Anlass, Anerkennung für das Geleistete auszusprechen – für eine kritische Auseinandersetzung und für mahnende Appelle in Zeiten, in denen Themen des Datenschutzes angesichts terroristischer Bedrohung nur eine untergeordnete Rolle zu spielen scheinen.

Insbesondere weil Ihre Organisation aus der Gesellschaft heraus und ehrenamtlich agiert, ist sie eine glaubwürdige, authentische und damit für den Datenschutz unverzichtbare Stimme. Hierfür möchte ich Ihnen, auch im Namen meiner Kolleginnen und Kollegen in der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, meinen Dank aussprechen. Ich wünsche Ihnen und uns, dass Sie auch in den kommenden Jahren ohne Scheu und mit anerkennenswerter Beharrlichkeit Probleme und Risiken im Datenschutz offen benennen und sich weiterhin engagiert für die Wahrung der Rechte der Bürgerinnen und Bürger einsetzen.



Zum 40jährigen Bestehen der DVD

Vor zehn Jahren gratulierte der damalige FIfF-Vorsitzende Hans-Jörg Kreowski der Deutschen Vereinigung für Datenschutz mit den folgenden Worten zum 30. Jubiläum:

„Wie nötig der Schutz vor Missbrauch personenbezogener Daten war und ist, zeigen die bis heute ungezählten Verstöße gegen den Datenschutz und die nicht minder häufigen Initiativen und Aktivitäten von Behörden, Polizei, Justiz, Ministerien und parlamentarischen Gremien, den Datenschutz zu unterlaufen, auszuhebeln und einzuschränken“,

und DVD-Vorstandsmitglied Thilo Weichert schrieb:

„Privatheit und Persönlichkeitsschutz sind eben nicht mehr Privilegien gehobener Gesellschaftsschichten, sondern eine Existenzbedingung einer demokratischen und rechtsstaatlichen Informationsgesellschaft. 30 Jahre Deutsche Vereinigung für Datenschutz sind hierfür noch nicht genug.“

Trotzdem erlebten wir auch in den vergangenen zehn Jahren ein stetig wachsendes Ausmaß an Überwachung und Datenschutzverletzungen. Die Enthüllungen von Edward Snowden zeigten uns, wie wir umfassend durch Geheimdienste wie die US-amerikanische NSA, das britische GCHQ oder den deutschen BND ausgespäht werden. Versuche, dies aufzuklären, laufen ins Leere; Befugnisse der Geheimdienste werden erweitert, rechtswidriges Handeln von Behörden gesetzlich legalisiert. Die Ergebnisse einer parlamentarischen Untersuchungskommission hat man nicht einmal abgewartet, bevor die nächsten, erweiterten Befugnisse für Sicherheitsbehörden verabschiedet wurden.

Doch auch der gesetzliche Datenschutz ist bedroht. Fortschritte der EU-Datenschutz-Grundverordnung werden bei der Anpassung an deutsches Datenschutzrecht konterkariert. Die deutsche Delegation – so hört man – habe sich als einer der größten Bremser bei der Fortschreibung des europäischen Datenschutzrechts erwiesen.

Vor uns stehen gleichzeitig große Herausforderungen. Unter dem Schlagwort Big Data und mit fortgeschrittenen Methoden und Techniken der Auswertung großer, unstrukturierter Datenmengen entstehen seit einiger Zeit neue Risiken. Unsere „analogen“ Aktivitäten werden in digitale Daten übersetzt und auswertbar gemacht, beispielsweise durch Sensoren oder mit Hilfe von Videoüberwachung. Basis für diese Digitalisierung ist das Smartphone, das die meisten von uns freiwillig (und gern) mit sich herumtragen. Unternehmen entwickeln neue Dienstleistungen und Geschäftsmodelle, die auf diesen Daten basieren. Gleichzeitig werden diese Dienste intensiv genutzt – sie erhöhen den Komfort, erleichtern unser tägliches Leben und eröffnen neue Möglichkeiten. In diesem Spannungsfeld muss der moderne Datenschutz Antworten finden und durchsetzen – eine Herkulesaufgabe, auch für die DVD.

Nicht zuletzt hat der Datenschutz auch eine politische Dimension: Er schützt Individuen gegen Übermacht und Willkür des Staates und von staatlichen und privaten Organisationen. Nicht umsonst sind beispielsweise Wahlen in unserer demokratisch verfassten Gesellschaft geheim. „Wissen ist Macht“ – und die umfassend über uns gesammelten Daten sind die Grundlage dieses Wissens.

Die DVD hat den Datenschutzdiskurs seit ihrer Gründung 1977 begleitet. Meilensteine des Datenschutzes fallen in die vergangenen 40 Jahre. Das erste deutsche Datenschutzgesetz 1977, das vom Bundesverfassungsgericht festgestellte Recht auf informationelle Selbstbestimmung 1983, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 2008 und die wiederholten höchstrichterlichen Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs gegen die Vorratdatenspeicherung – deren Konsequenzen von den politisch Verantwortlichen leider immer wieder vom Tisch gewischt werden – sind die symbolträchtigsten davon. Durch ihr unermüdliches Vorantreiben des Datenschutzes, durch Führen des Diskurses, durch berufliches Handeln und durch rechtliche Initiativen haben die DVD und ihre Mitglieder einen ent-

scheidenden Beitrag dazu geleistet.

Das FIfF – *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* –, als kritischer Berufsverband der Informatik, der 1984, also sieben Jahre später, gegründet wurde, versteht sich dabei als ein Partner der DVD. Unsere Ursprünge liegen in der Friedensbewegung der 1980er Jahre; unsere Arbeitsschwerpunkte sind breit gefächert und erstrecken sich über alle Themen, die die gesellschaftlichen Auswirkungen und verantwortliches Handeln in der Informatik berühren.

Der Datenschutz ist nach unserem Verständnis für dieses verantwortliche Handeln in der Informatik zentral. Datenschutz ist Menschenschutz; er ist die Voraussetzung für die verfassungsrechtlich garantierte Menschenwürde und die freie Entfaltung der Persönlichkeit. *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“*, führte das Bundesverfassungsgericht in seinem bahnbrechenden Volkszählungsurteil (BVerfGE 65, 1) 1983 aus und bestätigte damit die Bedeutung des Datenschutzes als deren unabdingbare Voraussetzung.

Damit ist der Datenschutz auch für das FIfF eins seiner wichtigsten Schwerpunktthemen, und so gab und gibt es immer wieder Gelegenheiten, gemeinsam für unsere Ziele zu arbeiten. Vor zehn Jahren trafen wir uns in Bielefeld, wo wir an einem Wochenende erfolgreiche Tagungen der DVD, des FIfF und die BigBrotherAwards erlebten und Bielefeld zur *Hauptstadt des Datenschutzes* machten. (Nebenbei: Dieses Zusammentreffen war für mich persönlich die Gelegenheit, auch Mitglied der DVD zu werden.) Drei Jahre später trafen wir uns in Köln zur gemeinsamen Jahrestagung. Ungezählt sind die Erklärungen und Forderungspapiere, die wir gemeinsam erarbeitet oder unterzeichnet haben. Wir teilen die Sorge über die zunehmende Überwachung aller Aspekte des Lebens durch staatliche Behörden und durch Wirtschaftsunternehmen, uns eint das gemeinsame Ziel, auch künftig einen effektiven Datenschutz sicherzustellen – juristisch wie technisch.

Die aktuellen Entwicklungen lassen nicht erwarten, dass uns die Arbeit in absehbarer Zeit ausgehen wird. Es gilt, ein effektives Datenschutzrecht und einen wirksamen technischen Datenschutz auch im Zeitalter von *Big Data* fortzuentwickeln und dem Datenhunger von Wirtschaftsunternehmen und ihren datenorientierten Geschäftsmodellen ebenso wie einer Sicherheitspolitik, die längst jedes Maß verloren hat, unsere alternativen Modelle entgegenzustellen. Das FIfF freut sich darauf, für diese Ziele weiterhin in einer starken Partnerschaft an der Seite der DVD zu arbeiten und zu streiten.

Auch 40 Jahre DVD sind noch bei weitem nicht genug! Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung gratuliert der Deutschen Vereinigung für Datenschutz zum 40jährigen Bestehen und wünscht ihr auch in Zukunft Engagement, Zivilcourage, Durchhaltevermögen, politische Kraft und vor allem: Erfolg für ihre Initiativen. Ein starker Datenschutz und eine starke DVD ist in unser aller Interesse.

Stefan Hügel
Vorsitzender des FIfF

Douwe Korff *

40TH BIRTHDAY WISHES FOR DVD & DANA

When the *Deutsche Vereinigung für Datenschutz e. V.* (DVD) was founded in 1977, and when the now famous *Datenschutz Nachrichten* were first published the next year, I was not yet really involved with data protection, but Amnesty International researcher for the then two Germanies (and the UK and Ireland) and “Head of Europe” at AI’s International Secretariat – and Amnesty’s mandate was limited and did not yet, as such, include privacy or surveillance.

However, as the person responsible for following human rights-related events in the Federal Republic of Germany generally, I quickly came into contact with lawyers and activists who not only fought against the draconian “anti-terror” laws then being introduced, but who also (rightly) saw data protection as a crucial new battlefield in that context – notably the sadly-missed Sebastian Cobler.

Over the next years, Sebastian and I had great discussions about the anti-liberal developments in the FRG at the time (*plus ça change* ...), over *Apfelwein* and *Handkäse (mit Musik!)* in Sachsenhausen. He had deep insights in the insidious ways in which seemingly minor changes to the criminal law, and court interpretations stretching on-their-face-innocuous rules, could corrupt the Rule of Law and German (now also European) constitutional principles – all illustrated with detailed references to how bad laws and bad legal approaches from the Weimar Era were taken up and further abused by the National Socialists – and then again picked up in the anti-communist campaigns in the ‘50s and ‘60s, and used for repressive actions against non-violent activists, and even academic observers of events, in those late-‘70s/early ‘80s. Remember the outrageous prosecutions of respectable academics for re-publishing the *Buback Nachruf*.[1]

The then newly-emerging idea of “data protection” (*Datenschutz*) as a fundamental right in Germany must be seen in that context. Politically active citizens objected to the census that was to be held in 1983, because they saw it as a tool to support the already excessive surveillance of activists and the clampdown on any expressions that the autho-

rities saw as being even remotely "sympathetic" to or "supportive" of political ideas and ideologies that were also invoked by the RAF. Sebastian Cobler was one of the lawyers acting in the case before the Constitutional Court, leading to the famous *Volkszählungsurteil (Census judgment)* of 15 December 1983.

By then, I had left Amnesty but was continuing to work for them as an academic, first at the Max Planck Institute for Criminal Law in Freiburg i.Br., and then briefly at the MPI for public law in Heidelberg. Although I focused on writing briefings for AI on international standards in criminal procedure, and on the "Diplock Courts" in Northern Ireland, and went to observe some trials for them (the *Sybille Haag* trial in Stuttgart-Stammheim, but also a trial in East Berlin), it was also at this time (in the early 1980s) that I was asked to advise AI on data protection: its collecting, analysing, sharing and publishing of often highly sensitive, and not always confirmed, personal data on political prisoners and victims of torture or extra-judicial killings, world-wide, was (and is) difficult to fit in with data protection rules that were not written with organisations such as AI in mind.

That is how I became involved in data protection in the early 1980s – and got to know all the great early data protection campaigners: apart from Sebastian Cobler, who I already knew from my work on criminal law, there was Professor Spiros Simitis in Frankfurt, the world's first data protection commissioner and a great data protection advocate (not only in the Hessen Parliament to which he formally reported, but also in the rest of Germany, and Europe). Also my countryman, Frits Hondius, who almost single-handedly wrote the 1981 Council of Europe Data Protection Convention, and Louis Joinet, the first President of the French data protection authority, the CNIL, who drafted the UN data protection guidelines and was looking into the AI issues.

In the data protection developments and battles that followed those early days – from the drafting of the 1995 EC Data Protection Directive and the 2001 e-Privacy Directive to the 2016 EU General Data Protection Regulation and the proposal for an e-Privacy Regulation – German law remained a major source of inspiration for the European data protection rules – partly because, as a result of the *Solange* decisions of the Karlsruhe court, the adoption of EU data protection rules that fell short of the German constitutional requirements would have re-opened the old debate about the supremacy of EU law. Strong data protection rules in Germany, and strong judgments in this field issued by the German Constitutional Court, are therefore crucial means to advance also the European standards in this area. The recent strong judgments of the CJEU on data protection-related matters clearly drew on the German case-law (and the Court was of course fully aware of the *Solange* implications).

But both in Germany and in Europe, there have also been attempts to weaken data protection. It is partly because of the concerted efforts of some principled German officials, in particular data protection authorities such as Thilo Weichert and Peter Schaar (both of course closely associated with DVD), and European civil servants (let me mention Ulf Brühann, Marie Georges and Sophie Kwasny, but above all the great Giovanni Buttarelli), human rights officials such as the Council of Europe Human Rights Commissioner, Nils Muižnieks, and his predecessor, Thomas Hammerberg, and parliamentarians committed to human rights and data protection such as Jan Albrecht and Sophie in 't Veld, that those efforts have been thwarted. However, they would all gladly acknowledge that in this they absolutely needed the backing of civil society and campaigning organisations with a sound reputation for critical but informed analysis.

In Europe, there is European Digital Rights (EDRi), led by the indefatigable Joe McNamee, and its many members and observers in many EU Member States (which include DVD). They have gained significant influence on the development of EU and Council of Europe data protection law.

In Germany, under Thilo Weichert's, Karin Schuler's, Sönke Hilbrans' and Frank Spaeing's leadership, and because of the major work by its members, DVD was and remains preeminent in this role (although there are now of course also other great organisations active on data protection and wider "digital" issues). I am honoured to have occasionally been asked to present my views on EU- and comparative-legal developments to DVD-organised fora, and in DANA.

The reason I dwelt somewhat on the wider context to my early recollections at the beginning of this note, is that I feel the clock has gone full circle: data protection, at some time seen as a rather *niche* interest at the margins of the wider human rights panorama, has again become closely and inextricably linked to the main human rights issues of today. As political activism, -organisation, -association and -speech have gone online, so have policing of such activities and mass surveillance. While few would argue against the need to counter hate speech and expressions of support for terrorism, also in the digital environment, once again the question is where and how to draw the line between this and respecting free speech and political action, and the extent to which state authorities should be allowed to interfere with those rights. But to the serious problems raised by this question in any one state, are now added the complexities of "cyberspace" not respecting state boundaries, and different states – including states that do not respect the rule of law; that oppress, torture and kill arbitrarily – acting and competing in that space; and of much of that space being under the control of private entities, including the US "Internet Giants".

Moreover, in "cyberspace" everything turns on data. Compulsory e-communications-, travel (PNR)-, financial and other data collection, -sharing and -retention; mass interception of communications, also extraterritorially; in-depth analyses of metadata, search queries, social- and communication networks; and the consequent "profiling" based on algorithms (including "dynamic", "self-learning" algorithms) – they are at the core of contemporary law enforcement and national security/ intelligence activities (which are moreover increasingly blurred, adding yet further complexity). And they are all about personal data (or results of analyses of supposedly non-personal data, but that are then used in relation to singled-out individuals). Decisions to impose travel bans, exclusions from jobs,

arrests and interrogation, and even becoming the target of killing drones – all are increasingly based directly or indirectly on such processing. Data protection is now at the centre of all major global human rights issues.

In the 1970s, DVD recognised this link, and was amongst the first in Europe to make it the focus of its civil society activities. It sustained this focus through the next decades. While there are now, fortunately, many other organisations, in Germany, Europe, the USA and globally, the work of the DVD remains crucial. It has provided through the years, and is still providing all the time (in particular through DANA), serious, in-depth, highest-quality analysis and criticism, with constructive engagement at the highest level. Trusted by law- and policy-makers and regulators, including the many German and other data protection authorities, it has never compromised on principles. It remains a much-needed voice – and I am sure will continue to make vital contributions to the debates on the various areas of concern I mentioned above.

I wish DVD a Happy 40th Birthday and a successful future! I feel privileged to have been involved with the organisation and with so many of its excellent members and leaders. In memory of Sebastian Cobler, I raise a glass of *Apfelwein* to you!

- o – O – o -

Douwe Korff
Cambridge, September 2017

* Douwe Korff is Emeritus Professor of International Law at London Metropolitan University; Associate of the Oxford Martin School, University of Oxford; Visiting Fellow at Yale University (Information Society Project); and Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Frankfurt/O and Berlin.
douwe@korff.co.uk

1 I summarised the situation in a Note I wrote for Amnesty International, Aspects of the law regarding freedom of expression in the Federal Republic of Germany (1983), later used (with my trial observation report on the case against Sybille Haag et al.) in the AI publication Prosecution for the exercise of the right to freedom of expression in the Federal Republic of Germany, AI Document EUR 23/02/85, London, 1985.



Grußwort für vierzig Jahre Deutsche Vereinigung für Datenschutz e.V.

Vierzig Jahre Deutsche Vereinigung für Datenschutz e.V. – Da denkt man unwillkürlich „Gab es Datenschutz da eigentlich schon?“ Nun gut, jetzt werden ältere Vereinsmitglieder sicher darauf hinweisen, dass ja beispielsweise das Hessische Datenschutzgesetz schon 1970 in Kraft trat. Aber das Datenschutz wichtig war, das war 1977 doch nun wirklich nur ein paar wenigen Fachleuten klar. Und die Notwendigkeit eines „Rechts auf informationelle Selbstbestimmung“, die hat auch kaum jemanden verstanden. Das lag ja aber vielleicht auch daran, dass nur wenige Menschen wussten, was Datenverarbeitung eigentlich tatsächlich ist und was sie kann. 1977 war nämlich auch das Jahr, in dem Ken Olsen, Gründer des einstmals mächtigen Computerkonzerns Digital Equipment (DEC) und „IT-Fachmann“, öffentlichkeitswirksam darlegte, dass niemand einen Computer zu Hause braucht. Den PET 2001 Personal Computer, den die Firma Commodore damals auf den Markt brachte, hielt Olsen sicher für einen Fehler.

Nun gut, Olsen hat sich getäuscht, DEC ist schon seit lange vom Markt verschwunden, wir sind von Datenverarbeitungen und Datensammlungen im beruflichen wie im privaten Bereich umzingelt und der Datenschutz wird gerade neue erfunden. Und da kommt nun wieder die Deutsche Vereinigung für Datenschutz e.V. ins Spiel. Das sie vor vierzig Jahren gegründet wurde, das war visionär. Aus heutiger Sicht ist es erfreulich, dass da nun eine anerkannte Institution existiert. Ihre Mitglieder haben vielfältige Erfahrungen zu den Risiken, die Datenverarbeitung für Bürgerinnen und Bürger mit sich bringen kann und wissen, wie diese ausgeschlossen oder minimiert werden können. Mit diesem Wissen macht die Deutsche Vereinigung für Datenschutz zu ihrem „Vierzigsten“ allen Bürgerinnen und Bürgern ein wichtiges Geschenk. Dafür vielen Dank!

Was wünscht man einer solchen Institution für die Zukunft? Dass es hier für Deutsche Vereinigung für Datenschutz viel Arbeit geben wird, liegt auf der Hand. In einer immer umfassender vernetzten und digital durchdrungenen Welt Datenschutz im Sinne der Nutzer sicherzustellen, dass wird anstrengend für die Menschen, die diese Vereinigung tragen und gestalten. Aber es lohnt sich weiterhin. In diesem Sinn wünsche ich Ihnen und Euch weiterhin die Energie, die es braucht, um die Vorteile der elektronische Datenverarbeitung für alle nutzbar zu machen und zugleich die Rechte von Bürgerinnen und Bürgern zu wahren. Alles Gute, Deutsche Vereinigung für Datenschutz.

Prof. Dr. Peter Wedde

Professor für Arbeitsrecht und Recht der Informationsgesellschaft im FB 2 Informatik und Ingenieurwissenschaften an der Frankfurt University of Applied Sciences und wissenschaftlicher Leiter des Instituts für Datenschutz, Arbeitsrecht und Technologieberatung in Eppstein / Taunus.

Bernd Schütze

Controlling der IT-Sicherheit unter Berücksichtigung von Art. 32 Datenschutz-Grundverordnung

Art. 32 Datenschutz-Grundverordnung (DS-GVO) schreibt vor, dass sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden – der Auftragsverarbeiter unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zugleich resultiert aus Art. 5 DS-GVO eine Nachweispflicht. Damit lässt sich festhalten:

1. Der Schutz der Daten ist nicht absolut. Es muss aus datenschutzrechtlichen Gründen nicht zwingend das höchstmögliche Schutzniveau umgesetzt werden, sondern ein unter Berücksichtigung der oben genannten Punkte angemessenes Niveau.
2. Es existiert bzgl. der Angemessenheit eine Nachweispflicht.

Was ist „Stand der Technik“?

In der DS-GVO existiert keine Legaldefinition bzgl. „Stand der Technik“. in der Begründung zum IT-Sicherheitsgesetz[1] heißt es:

„Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.“

Aus europäischer Sicht bietet am ehesten der Terminus „beste verfügbare Technik“ entsprechend Art. 3 Ziff. 10 Industrieemissions-Richtlinie[2] eine Definition bzgl. „Stand der Technik“. Hier findet sich als Definition

„beste verfügbare Techniken“ den effizientesten und fortschrittlichsten Entwicklungsstand der Tätigkeiten und entsprechenden Betriebsmethoden, der bestimmte Techniken als praktisch geeignet erscheinen lässt, […] oder, wenn dies nicht möglich ist, zu vermindern:

a) „Techniken“: sowohl die angewandte Technologie als auch die Art und Weise, wie die Anlage geplant, gebaut, gewartet, betrieben und stillgelegt wird;
b) „verfügbare Techniken“: die Techniken, die in einem Maßstab entwickelt sind, der unter Berücksichtigung des Kosten/Nutzen-Verhältnisses die Anwendung unter in dem betreffenden industriellen Sektor wirtschaftlich und technisch vertretbaren Verhältnissen ermöglicht, gleich, ob diese Techniken innerhalb des betreffenden Mitgliedstaats verwendet oder hergestellt werden, sofern sie zu vertretbaren Bedingungen für den Betreiber zugänglich sind;
c) „beste“: die Techniken, die am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus […] sind“.

Übertragen auf die IT-Sicherheit folgt daraus: unter Berücksichtigung des Kosten/Nutzen-Verhältnisses muss die Technik eingesetzt werden, welche für den jeweiligen Bereich als Standard angesehen wird und dabei das höchstmögliche Schutzniveau gewährt. Wikipedia beschreibt den Begriff „Standard“ wie folgt: „Ein Standard ist eine vergleichsweise einheitliche oder vereinheitlichte, weithin anerkannte und meist angewandte (oder zumindest angestrebte) Art und Weise, etwas herzustellen oder durchzuführen, die sich gegenüber anderen Arten und Weisen durchgesetzt hat.“[3]

Stand der Technik und Normen

Normen und Richtlinien sind in erster Linie Empfehlungen privater Vereine, z.B. die vom Deutschen Instituts für Normung (DIN) herausgegebenen Normen. Die Verbindlichkeit einer Norm regelt sich durch die Vereinbarung der beteiligten Parteien, für welche die Norm(en) Leistungsgrundlage sein soll. Somit stellen Normen nicht zwangsläufig eine Regel oder Stand der Technik dar. Vielmehr ist eine Norm dann anerkannt, wenn Fachleute diese anwenden und sich dabei sicher sind, dass sie dem Stand der Technik entspricht. Dies beinhaltet, dass die Norm „gepflegt“ wird, d.h. regelmäßig aktuell gehalten wird.

Ist die Anwendung von bestimmten Normen in einer Rechtsvorschrift vorgeschrieben, so ist deren Einhaltung selbstverständlich auch verpflichtend, auch wenn diese ggf. nicht mehr dem Stand der Technik entsprechen.

Nachweis „angemessene Maßnahmen“

Bei der Auswahl der Maßnahmen sind die „Implementierungskosten“ zu berücksichtigen. Dies bedingt eine betriebswirtschaftliche Bewertung von Maßnahmen der Informationssicherheit. Hierzu ist einerseits die vollständige Erfassung und adäquate Quantifizierung der bestehenden Risiken erforderlich, andererseits müssen die Kosten und Wirksamkeit von Schutzmaßnahmen dargestellt werden. Schwierig hieran ist, dass gerade im Bereich der IT-Sicherheit häufig eine

hinreichend präzise Quantifizierung der Risiken nicht möglich ist; hier muss eine bestmögliche Näherung erzielt werden.

Identifizierung der Risiken

In der DS-GVO geht es darum, den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger von der Verarbeitung betroffener Menschen Rechnung zu tragen. Entsprechend adressiert Art. 32 DS-GVO mit seinen Anforderungen die Risiken für die betroffenen Personen, Risiken für das datenverarbeitende Unternehmen sind nur relevant, wenn diese zugleich auch Risiken für die von der Verarbeitung betroffenen Personen darstellen.

Eine Kategorisierung der Risiken für die Rechte und berechtigten Interessen betroffener Personen bei einer Verarbeitung personenbezogener Daten können z. B. sein[4]:

- Strukturelle Risiken, beispielsweise gesellschaftlich-politische Risiken (wie z. B. die Informationsmacht, die gegenüber einem Individuum gewonnen wird) oder wirtschaftliche Risiken
- Individuelle Risiken, wie z. B. die Erhöhung individueller Verletzlichkeit für Straftaten, da jemand erfährt, wo betroffene Personen angreifbar sind
- Risiken für Gesellschaft und Individuum, z.B. durch Bildung von Persönlichkeitsprofilen oder Fremdbestimmung oder auch die Enttäuschung von Vertraulichkeitserwartungen.

Die Risiken für die betroffenen Personen können aus Sicht der IT-Sicherheit i. d. R. auf drei Fälle eingegrenzt werden:

1. Unbefugte erhalten Zugriff auf die Informationen
2. Informationen erfahren eine unerwünschte Änderung
   2.1. Dies geschieht ungewollt durch einen Anwender, dem entsprechend Rechte zugewiesen wurde (z. B. Fehlbedienung oder Unachtsamkeit)
   2.2. Dies geschieht durch einen Angreifer, der sich entsprechende Rechte verschaffte
3. Informationen werden vernichtet.
   3.1. Dies geschieht ungewollt durch einen Anwender, dem entsprechend Rechte zugewiesen wurden (z. B. Fehlbedienung oder Unachtsamkeit)
   3.2. Dies geschieht durch einen Angreifer, der sich entsprechende Rechte verschaffte

Quantifizierung der Risiken

Eine Quantifizierung erkannter Risiken kann u. a. durch die nachfolgend vorgestellten vier Ansätze erfolgen:

1. Experten-Befragung: Mit Hilfe von meist strukturierten Fragebögen wird versucht, IT-Sicherheitsrisiken zu identifizieren und zu quantifizieren.
2. Indikator-Ansatz: Anhand bestimmter Kennzahlen bzw. eines Kennzahlensystems werden vorliegende IT-Sicherheitsrisiko indirekt ermittelt.
3. Stochastische Methoden: Basierend auf historischen Schadensdaten bzgl. der Häufigkeit und Schwere von eingetretenen Schäden werden statistische Verteilungsfunktionen zur Simulation genutzt, um so das Eintreten künftiger IT-Sicherheitsrisiken abzuschätzen.
4. Kausal-Methoden: Zwischen den identifizierten Risikoquellen bzw. -treibern und den daraus resultierenden Schäden werden mittels statistischer Methoden Zusammenhänge dargestellt.

Betriebswirtschaftliche Betrachtung

Für diese betriebswirtschaftliche Abwägung und Maßnahmenbewertung wird in der Praxis häufig der Return on Security Investment (RoSI) als Kennzahl eingesetzt. Die Rentabilität einer IT-Sicherheitsmaßnahme wird anhand eines Vergleichs des gesenkten IT-Sicherheitsrisikos durch die Implementierung einer IT-Sicherheitsmaßnahme mit den Kosten für die Maßnahme ermittelt.

Hierzu ist es zunächst erforderlich den zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE) zu bestimmen. Der ALE errechnet sich aus der finanziellen Höhe (Loss, L) und der Eintrittswahrscheinlichkeit (Probability, P) eines potentiellen Schadens: $ALE = L \cdot P$.

Der zu erwartende Gesamtverlust ist dann die Summe der Erwartungswerte aller betrachteten Einzelrisiken: $ALE_{tot} = \sum_{i=1}^{n} L_i \cdot P_i$.

Die Reduktion eines betriebswirtschaftlichen Risikos kann einerseits durch eine Verringerung der Eintrittswahrscheinlichkeit erfolgen, andererseits durch eine Begrenzung der Auswirkungen des Schadens. Für das „klassische" Controlling der IT-Sicherheit steht beides gleichberechtigt nebeneinander. Art. 32 DS-GVO verlangt jedoch eine Begrenzung des Risikos für die betroffene Person. D.h. wenn durch Maßnahmen das finanzielle Risiko z.B. durch verhängte Bußgelder reduziert wird, das Risiko für die betroffene Person unverändert ist, so ist dies keine risikoreduzierende Maßnahme aus Sicht des Art. 32 DS-GVO. (Gleichwohl kann die Ergreifung der Maßnahme aus Sicht des die Daten verarbeitenden Unternehmens natürlich wünschenswert sein.)

Leider existieren für die wenigsten Schäden im Bereich der IT belastbaren Erfahrungswerte, so dass die Berechnung des ALE-Wertes nur als Schätzung erfolgen kann. Berücksichtigt werden müssen bei der Kalkulation eines zu erwartenden Verlustes insbesondere

- Umsatzeinbußen, z.B. durch Ausfall eines Shopsystems
- Produktivitätskosten, wenn beispielsweise durch den Ausfall Produkte nicht weiterentwickelt werden können
- Wertverlust, z.B. durch Imageschaden
- Wiederherstellungskosten
- Schadensersatzleistungen, z.B. gegenüber betroffenen Personen
- Sanktionsmaßnahmen, wie z.B. von Aufsichtsbehörden verhängte Bußgelder.

Kostenart	Kosten
Wiederherstellungskosten:	
(externer Berater (4 Stunden, Stundensatz 250 Euro)	1.000,00 €
Umsatzeinbußen	
(0,5 Aufträge /Stunde Ausfall (pro Auftrag ~ 5.600 Euro)	11.200,00 €
Produktivitätskosten:	
(12 Beschäftigte im Marketing (Ausfall 4 Stunden, Stundenlohn 18,60 Euro)	892,80 €
(Fax statt Mailbestätigung für eingegangene Aufträge (25 x, Kosten je Fax 0,10 Euro)	2,50 €
Kosten einmaliger Ausfall:	13.095,30 €

Auch die Kosten für die Implementierung einer Schutzmaßnahme setzen sich aus unterschiedlichen Kostenblöcken zusammen:

- Konzeptionskosten, z.B. Entwicklung bzw. Auswahl der Lösung, Testbetrieb, Anpassungen an die eigene Infrastruktur
- Investitionskosten, wie beispielsweise anzuschaffende Hardware, Software, Schulungskosten, Installation/Konfiguration
- Betriebskosten, Kosten für Support. Lizenzkosten, usw.

Aus diesen drei Kostenblöcken werden die Gesamtkosten der Sicherheitsmaßnahmen (Total Cost of Ownership, TCO) berechnet. Hierbei ist zu beachten, dass Einmalkosten über den Betriebszeitraum abgeschrieben werden: $TCO = \frac{Konzeptionskosten + Investitionskosten}{Betriebszeitraum} + Betriebskosten$.

Der Return on Security Investment (RoSI) berechnet sich jetzt dadurch, dass der ALE-Wert vor und nach Einführung der IT-Sicherheitsmaßnahmen betrachtet wird: $RoSI = \frac{(ALE_{alt} - ALE_{neu}) - TCO}{TCO}$. Oder in Worte gefasst: die erwartete Ersparnis beim ALE-Wert $(ALE_{Alt} - ALE_{neu})$ muss über den Anschaffungs- und Betriebskosten liegen, dann ist die Maßnahme aus betriebswirtschaftlicher Sicht sinnvoll.

Diskussion

Im Berechnungsansatz wird vereinfachend davon ausgegangen, dass ein Risiko von einer Sicherheitsmaßnahme adressiert wird. In der Praxis adressiert eine Maßnahme häufig mehr als ein Sicherheitsrisiko, z.B. soll eine Firewall Denial-of-Service-Attacken ebenso verhindern wie das Eindringen Unbefugter in das eigene Rechnernetz. Andererseits können Maßnahmen auch neue Risiken in sich bergen, z.B. muss zur Fernwartung Dritten Zugriff auf das eigene Rechnernetz gewährt werden, was grundsätzlich einen potentiellen Missbrauch des Zugangs beinhaltet (z.B. durch einen Zugriff Unbefugter auf das Netz der fernwartenden Partei) und somit immer auch eine Sicherheitslücke darstellt. Weiterhin wird davon ausgegangen, dass eine Schadenswiederholung einen gleichbleibenden Schaden verursacht. Jedoch wird ein einmaliger Sicherheitsvorfall in einer Bank oder einem Krankenhaus durch die Öffentlichkeit anders bewertet, als wenn einmal pro Monat ein entsprechender Vorfall passiert, was wiederum in einem gesteigerten Imageverlust resultiert. Ferner besteht der „Gewinn" in der Betrachtung in einer Verminderung eines operationellen Risikos, also eines Erwartungswertes für die Kosten von Sicherheitsvorfällen; ob dadurch tatsächlich Einsparungen erzielt worden sind, lässt sich selbst nachträglich nach Eintritt eines Schadensfalls selten feststellen.

D.h. die Abschätzung wird sicherlich nicht die Wirklichkeit widerspiegeln, jedoch kann RoSI die Tendenz recht gut darstellen. Daher erscheint RoSI gut geeignet, um für Dritte wie z.B. Aufsichtsbehörden nachvollziehbar darlegen zu können, warum Investitionskosten für IT-Sicherheitsmaßnahmen für ein Unternehmen tragbar sind oder nicht.

1 Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). S. 14, 15. Online, zitiert am 2017-08-31; Verfügbar unter https://dip21.bundestag.de/

2 Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24. November 2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung). Online, zitiert am 2017-08-31; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32010L0075

3 Wikipedia „Standard". Online, zitiert am 2017-08-31; Verfügbar unter https://de.wikipedia.org/wiki/Standard

4 Stefan Drackert (2014) Die Risiken der Verarbeitung personenbezogener Daten - Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN ,978-3-428-1 4730-4

Riko Pieper

Kuriositäten in der [Datenschutz-]Gesetzgebung

Einleitung

„Datenschutzbeauftragter" (DSB) ist keine Berufsausbildung, sondern etwas, wozu man „benannt"[1] wird. In der Praxis haben Datenschutzbeauftragte vor der Datenschutzausbildung daher meistens ein Studium abgeschlossen, das wenigstens einen Teil der Aufgaben eines DSB abdeckt. Die Aufgaben eines DSB[2] bestehen einerseits darin, die jeweiligen Mitarbeiter und die oberste Leitung des Unternehmens in datenschutzrechtlichen Fragen zu beraten, andererseits in Überprüfungen der Prozesse und IT-Systeme des Unternehmens auf Konformität in Bezug auf die datenschutzrechtlichen Vorgaben. Daher ist es nicht verwunderlich, dass Datenschützer oft entweder Juristen oder Informatiker sind oder ein diesen beiden Disziplinen verwandtes Studium abgeschlossen haben, denn der Datenschutz verbindet beides.

In diesem Artikel werden einige Tücken in der Gesetzgebung beschrieben, die der Autor in seiner Rolle als Datenschützer[3] und Informatiker gefunden und mit anderen Datenschützern[4] diskutiert hat. Die Ergebnisse waren ernüchternd. Teilweise handelt es sich um offensichtliche „Fehler" im Gesetz, die allgemein bekannt zu sein scheinen und trotzdem selbst bei Gesetzesänderungen nicht be-

hoben wurden. Teilweise handelt es sich aber auch um bisher weniger bekannte Fälle von missverständlichen Formulierungen, die zu Fehlinterpretationen führen können und bereits geführt haben[5].

Es soll nicht der Eindruck entstehen, dass Informatiker die besseren Juristen sind. Es ist aber vielleicht auch kein Zufall, dass dieser Artikel von einem Informatiker geschrieben wurde, denn die im Folgenden beschriebenen Probleme sind weitgehend auch in der Informatik bekannt. Teilweise gibt es dort dafür hilfreiche Methoden, um sie zu lösen oder wenigstens erkennen zu können oder im besten Fall von vornherein zu vermeiden bzw. gar nicht zu ermöglichen[6].

Dieser Artikel beschreibt elf Beispiele, die sich ausnahmslos auf das Datenschutzrecht (alt und neu) beziehen, was damit zu tun hat, dass sich der Autor – wie oben beschrieben – als Datenschützer speziell mit diesem Teil des Rechts befasst hat. Die Beispiele erheben daher keinen Anspruch auf Vollständigkeit.

Die Beispiele beziehen sich auf folgende Themen:

I. Begriffe / Definitionen
II. Toter Code
III. Sprachwirrwarr

Teil I: Begriffe / Definitionen

Erläuterung

Das Datenschutzrecht enthält unterschiedliche Varianten von Problemen mit Begriffen und Definitionen. Zum einen gibt es ungünstige bzw. missverständliche Definitionen (1., 4. und 5. Beispiel). Andererseits fehlen häufig Definitionen von Begriffen, für die es aber klare Vorstellungen gibt (1. und 2. Beispiel). Ferner existieren Wortvarianten von definierten Begriffen, bei denen man darüber streiten kann, ob es sich nur um einen anderen Ausdruck für einen klar definierten Begriff handelt oder um etwas ganz Anderes (1. und 3. Beispiel). Es kann aber auch passieren, dass eine Unklarheit durch eine Übersetzung entsteht (4. und 5. Beispiel), was aber nicht bedeuten muss, dass das Original aussagekräftiger war (5. Beispiel). Die folgenden Beispiele erläutern von allem etwas. Die meisten fallen sogar in mehrere der oben genannten Kategorien.

1. Beispiel: Was bedeutet „schriftlich"?

Dieses erste Beispiel zeigt bereits, dass es nicht ausschließlich um das Datenschutzrecht geht, denn der Begriff „schriftlich" kommt auch in vielen anderen Gesetzen vor. Man sollte also annehmen, dass er klar definiert ist. Wenn man Juristen danach fragt, bekommt man oft die Antwort, dass „schriftlich" immer „Schriftform" bedeutet und die Schriftform im § 126 BGB definiert ist. Damit ist der Fall dann klar.

Ganz so klar ist der Fall aber dann doch nicht, weil es Fälle gibt, in denen allgemein argumentiert wird, dass hier keine formale „Schriftform" erforderlich ist.[7]

Als Beispiel für die Auslegung von „schriftlich" im Sinne von „Schriftform" kann der § 11 Abs. 2 Satz 2 BDSG-alt genannt werden:

„Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:"

Obwohl dort „schriftlich" steht, kann man überall nachlesen, dass der hier beschriebene ADV-Vertrag in „Schriftform" vorliegen muss.

Anders sieht es mit § 28 Abs. 3a BDSG-alt aus:

„Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann."

Interessant – und gleichzeitig ein Argument für die andere Auslegung des Begriffes „schriftlich" – ist, dass hier in einem Satz beide Begriffe „Schriftform" und „schriftlich" vorkommen. Bei der Auslegung dieses Absatzes wird allgemein argumentiert, dass eine Bestätigung einer nicht in Schriftform erteilten Einwilligung zwar zu erfolgen hat – diese aber nicht die „Schriftform" erfüllen muss; denn anderenfalls hätte man hier auch explizit „Schriftform" geschrieben.

Diese Auslegung macht unter praktischen Gesichtspunkten Sinn. Wenn man in einem Prozess eine große Anzahl von Einwilligungen einholen würde, die nicht in „Schriftform" vorliegen würden und diese dann alle z. B. auf dem Postweg in „Schriftform" bestätigen müsste, dann müsste es Angestellte geben, die wie am Fließband diese Anschreiben unterschreiben. Das würde man so kaum umsetzen. Man würde mit eingescannten Unterschriften arbeiten, wie das oft der Fall ist. Solche Schreiben erfüllen aber per Definition nach § 126 BGB **keine** „Schriftform". Die Schriftform macht hier nur bei den Einwilligungen selbst Sinn, denn damit hätte man einen Beweis für die Einwilligung. Die Bestätigung in „Schriftform" beweist gar nichts.

Wenn es aber stimmt, dass „schriftlich" in diesem Fall nicht „Schriftform" bedeutet, dann muss die Frage erlaubt sein, warum an anderer Stelle im gleichen Gesetz (und in anderen Gesetzen) „schriftlich" wie selbstverständlich als „Schriftform" zu interpretieren ist.

Das Problem der Interpretation von „schriftlich" wird in die neue Rechtsprechung übernommen. Im Art. 28 Abs. 9 DS-GVO steht:

„Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann."

Diese Formulierung lässt zunächst vermuten, dass „schriftlich" auch etwas Anderes als „Schriftform" bedeuten kann. Ganz eindeutig ist das aber nach wie vor nicht, denn man könnte argumentieren, dass das „elektronische Format" auch mit der „elektronischen Form" nach § 126a BGB erfüllt ist, die wiederum nach § 126 BGB die Schriftform erfüllt.

Die Beantwortung der Frage, was „schriftlich" genau bedeutet, ist keine Bagatelle, denn es kann einen deutlichen Aufwandsunterschied bei Prozessen ausmachen, ob die Dokumente in „Schriftform" vorliegen müssen oder nicht.

2. Beispiel: Privileg der Auftragsdatenverarbeitung (ADV)

Das „Privileg der ADV" besteht darin, dass ein Auftraggeber (Verantwort-

liche Stelle) im Falle einer ADV keine Rechtsgrundlage für eine Übermittlung der Daten an den Auftragnehmer braucht.

Dieses „Privileg der ADV“ ist weder im BDSG-alt noch in der DS-GVO definiert, es ist in beiden jedoch enthalten. Im BDSG-alt kann es aus den Definitionen der Begriffe „übermitteln“ und „Dritter“ hergeleitet werden, in der DS-GVO ist es leider nicht so einfach – gelten soll es dort aber trotzdem.[8]

Der eigentliche Paragraf zur ADV ist der § 11 BDSG-alt *„Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag“*. Dieser Paragraf 11 enthält keine Aussage darüber, ob ein Auftraggeber seine Daten an einen Auftragnehmer weitergeben[9] darf oder ob er dafür eine Rechtsgrundlage braucht. Die Antwort auf diese Frage erschließt sich aus folgenden Definitionen:

Im § 3 Abs. 4 Nr. 3 BDSG-alt wird „übermitteln“ definiert als:

„das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,“

Im § 3 Abs. 8 BDSG-alt wird „Dritter“ folgendermaßen definiert:

„Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.“

Ein Auftragnehmer einer ADV ist also laut der Definition für „Dritte“ kein Dritter, und eine Übermittlung findet per Definition immer an „Dritte“ statt, sodass es sich bei einer Weitergabe von Daten im Rahmen einer ADV nicht um „Übermittlung“ handelt, was wiederum zur Folge hat, dass man keine Rechtsgrundlage für eine Übermittlung braucht.

Das ist zwar um mehrere Ecken gedacht, scheint aber nachvollziehbar zu sein. Bei genauerer Betrachtung gibt es mit diesem Konstrukt jedoch große praxisrelevante Probleme. Das „Privileg der ADV“ gilt nämlich nicht grundsätzlich. Es gilt nur für *„Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.“*

Man wollte offensichtlich vermeiden, dass über das Konstrukt der ADV auch Daten an Auftragnehmer in (unsicheren) Drittstaaten weitergegeben werden können, denn die Einschränkung die dafür gelten, beziehen sich ja auch auf „Übermittlungen“ und bei einer ADV würde es sich ja nicht um „Übermittlung“ handeln. Übersehen wurde dabei, dass es auch eine Reihe von „sicheren Drittstaaten“ gibt, denen die EU-Kommission ein „angemessenes Datenschutzniveau“ bescheinigt hat. Aufgrund der oben angegebenen Definition entfällt das Privileg der ADV trotz des von offizieller Stelle bescheinigten angemessenen Datenschutzniveaus auch bei den sicheren Drittstaaten. Wenn man z. B. einen ADV-Vertrag mit einem Auftragnehmer in der Schweiz[10] abschließt, dann braucht man zusätzlich noch eine Rechtsgrundlage für eine „Übermittlung“.

Als Rechtsgrundlage wird in solchen Fällen oft § 28 *„Datenerhebung und -speicherung für eigene Geschäftszwecke“* Abs. 1 BDSG-alt herangezogen. Diese Rechtsgrundlage ist jedoch einerseits ein ganz dünnes Brett, was hier aber nicht weiter diskutiert werden soll. Andererseits gilt der § 28 Abs. 1 BDSG-alt auch nur für *„nicht-öffentliche Stellen“*.

Der Abschnitt 2 BDSG-alt für „öffentliche Stellen“ mit den §§ 12 bis 26 enthält keine entsprechende Rechtsgrundlage für „eigene Geschäftszwecke“, denn öffentliche Stellen haben keine eigenen Geschäftszwecke zu haben, sondern nur ihren jeweiligen gesetzlichen Auftrag zu erfüllen. Ob das immer so passt, sei hier einmal dahingestellt. Auf jeden Fall kann es bei öffentlichen Stellen wie bei jeder nicht-öffentlichen Stelle vorkommen, dass Auftragnehmer im Rahmen einer ADV einzubinden sind.

Das bedeutet, dass öffentliche Stellen bisher ADV-Verträge weder mit Auftragnehmern in (unsicheren) Drittstaaten[11] noch mit Auftragnehmern in sicheren Drittstaaten abschließen können. Ersteres könnte aufgrund der Snowden-Veröffentlichungen noch gewollt gewesen sein, wenn diese Beschränkung nach dessen Veröffentlichungen ins Gesetz gekommen wäre; für Auftragnehmer in sicheren Drittstaaten ist das gar nicht nachvollziehbar.

Mit der DS-GVO wird das zum Glück anders. Dort gibt es die unselige Verquickung in der Definition von „Dritten“ nicht mehr in Abhängigkeit von dem Land, in dem sich der Dritte befindet bzw. die Daten verarbeitet (siehe Art. 4 Nr. 10 DS-GVO). An anderer Stelle (ErwG. 48 DS-GVO – siehe auch 3. Beispiel) wird dann klargestellt, dass die Vorgaben für Drittländer trotzdem zu beachten sind, womit dann alles gut ist.

Im Bereich der Informatik kennt man in diesem Zusammenhang Begriffe wie Kopplung[12] und Kohäsion[13] (Bindung). Angestrebt wird eine starke Bindung innerhalb einer logischen Einheit, jedoch eine lose Kopplung zu anderen Einheiten, um die Abhängigkeiten und daraus resultierende Seiteneffekte zu minimieren. Im oben angegebenen Beispiel verursacht die Definition von „Dritter“ eine starke Kopplung und somit eine Abhängigkeit zu einem Thema, das damit eigentlich nichts zu tun hat, nämlich, dass es (unsichere) Drittstaaten gibt, bei denen ein angemessenes Datenschutzniveau sichergestellt sein muss, bevor die Daten dort erhoben, verarbeitet oder genutzt werden dürfen.

3. Beispiel: Unternehmensgruppe, Konzern, Konzernprivileg

Im BDSG-alt sind alle drei Begriffe nicht definiert. Das klingt zunächst konsequent, weil es kein Konzernprivileg gibt. Manche Unternehmen – insbesondere die ganz großen in den USA ansässigen Konzerne – verhalten sich jedoch oft so, als ob es ein Konzernprivileg gäbe. An dieser Stelle wäre es hilfreich, wenn es im Gesetz eine klare Aussage darüber gäbe, was es explizit nicht gibt.

Wenn z. B. ADV-Verträge mit einem Unternehmen in Europa abgeschlossen werden (siehe 2. Beispiel), dann werden dort typischerweise weitere Unterauftragnehmer angegeben und eine Über-

mittlung in Drittstaaten ausgeschlossen. Manche dieser Verträge enthalten eine harmlos aussehende Klausel, wonach die Weitergabe der Daten innerhalb des Konzerns davon ausgeschlossen ist.

Das ist jedoch genau das Konzernprivileg, das es nicht gibt! Wenn es sich dann außerdem noch um einen Konzern mit Niederlassungen bzw. sogar der Konzernmutter in einem (unsicheren) Drittstaat handelt, dann ist das gesamte Konstrukt der ADV und des damit verbundenen Privilegs (siehe 2. Beispiel) aufgehoben.

Die Juristen dieser Konzerne – von denen man weiß, dass sie es besser wissen – argumentieren gern damit, dass das kein Problem sei, weil der Konzern ja dem Safe Harbor Abkommen bzw. inzwischen dem EU-US Privacy Shield beigetreten ist.

In der DS-GVO ist der Begriff „Unternehmensgruppe“ nun im Art. 4 Nr. 19 folgendermaßen definiert:

„eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“

Unter Berücksichtigung des Erwägungsgrunds 37 DS-GVO ist eine Unternehmensgruppe nach dieser Definition zwar nicht unbedingt ein Konzern, aber ein Konzern kann nach dieser Definition in jedem Fall als Unternehmensgruppe angesehen werden. Ursprünglich soll auch ein Konzernprivileg in der DS-GVO geplant gewesen sein, das dann aber in der Verhandlungsphase wieder herausgenommen wurde. Die Definition der Unternehmensgruppe ist jedenfalls geblieben, und sie wird auch an einigen Stellen – wenn auch selten – benutzt.

Relevant könnte der Begriff der Unternehmensgruppe im Zusammenhang mit Art. 6 *„Rechtmäßigkeit der Verarbeitung“* Abs. 1 lit. f) DS-GVO werden:

„(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

…

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Hier kommen zwar die Begriffe „Unternehmensgruppe“, „Konzern“ oder „Konzernprivileg“ nicht vor, aber im Zusammenhang mit Erwägungsgrund 48 DS-GVO hat sich das Konzernprivileg nun doch durch die Hintertür – jedenfalls im Ansatz – eingeschlichen.

ErwG. 48 DS-GVO lautet:

„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.“

Immerhin ist im letzten Satz (wie im 2. Beispiel bereits erwähnt) die Einschränkung vorgegeben, dass die Vorgaben in Bezug auf Übermittlung in (unsichere) Drittstaaten davon unberührt bleiben.

Interessant und an dieser Stelle ausdrücklich erwähnenswert ist auch eine Stelle, an welcher der Begriff der „Unternehmensgruppe“ in der DS-GVO **nicht** steht, obwohl er ja definiert ist:

Gemeint ist Art. 83 Abs. 4 und 5 DS-GVO, der allgemein[14] dahingehend interpretiert wird, dass Konzerne mit Geldbußen von bis zu 2% bzw. 4% des weltweiten Vorjahresumsatzes rechnen müssen.

Art. 83 Abs. 4 DS-GVO lautet:

„Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:“

Absatz 5 unterscheidet sich von Absatz 4 nur in den Beträgen (20 Millionen € statt 10 Millionen € und 4% statt 2%) sowie in den hinter dem Doppelpunkt folgenden Unterpunkten.

In beiden Absätzen steht das Wort „Unternehmen“ und nicht das Wort „Unternehmensgruppe“!

Die Formulierung *„seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs“* lässt zwar vermuten, dass damit der gesamte Konzern gemeint ist, und so wird es ja auch allgemein gesehen. Es geht hier aber um sehr viel Geld. Bei den ganz großen Konzernen, deren Geschäftsmodell hauptsächlich darin zu bestehen scheint, die datenschutzrechtlichen Vorgaben zu ignorieren, kann es sich dann durchaus um hohe zwei- bis evtl. sogar dreistellige Millionenbeträge handeln. Bei solchen Beträgen wird man keine Mühen und Kosten scheuen und mit einer Heerschar von Anwälten versuchen zu begründen, weshalb sich diese Absätze des Art. 83 DS-GVO nicht auf den Konzern beziehen können. Man stellt sich als naiver Datenschützer schon die Frage, wie es sein kann, dass hier der definierte Begriff nicht genutzt wurde, obwohl er doch angeblich gemeint war.

Mancher Leser könnte daher die Erwähnung dieses Beispiels in einem Artikel über „Kuriositäten“ als geschmacklose Untertreibung interpretieren.

4. Beispiel: englisch: „Fairness“ – deutsch: „Verarbeitung nach Treu und Glauben“

In der englischen (Verhandlungs-) Sprache der DS-GVO ist in den Grundsätzen in Art. 5 „fairness“ erwähnt. In der deutschen Übersetzung steht „Verarbeitung nach Treu und Glauben“.

Die Begriffe „fair“, „fairness“ bzw. „Fairness“ stehen seit langer Zeit im deutschen Duden. Während man davon ausgehen kann, dass jeder, der Deutsch spricht, sich etwas darunter vorstellen kann, kann man sich da bei *„Verarbeitung nach Treu und Glauben“* nicht so sicher sein. Hier handelt es sich um einen juristischen Begriff, der aus dem „Bürgerlichen Gesetzbuch“ (BGB) kommen soll[15] und entsprechend hauptsächlich Juristen bekannt ist.

Wenn man sich die Mühe macht und im BGB danach sucht, dann findet man nur sieben Paragrafen[16], in denen der Begriff benutzt wird. In nur einem Paragrafen kommt der Begriff bereits im

Titel vor, sodass dies evtl. als Definition herangezogen werden kann:

§ 242 *„Leistung nach Treu und Glauben"* BGB lautet:
„Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern."

Was das genau bedeutet und was es zur Klarheit beiträgt, soll hier nicht näher betrachtet werden. Es scheint jedenfalls nichts Unanständiges zu sein.

5. Beispiel: englisch: „Controller" – deutsch: „Verantwortlicher"

Die Begriffe für die in einer Auftragsdatenverarbeitung (ADV)[17] vorkommenden Rollen von Auftraggeber und Auftragnehmer sind in der DS-GVO definiert als „Verantwortlicher" (Art. 4 Nr. 7) und als „Auftragsverarbeiter" (Art. 4 Nr. 8). Die Rolle des „Verantwortlichen" wird an vielen Stellen auch ohne Auftragsverhältnis genutzt, sodass nachvollziehbar ist, warum man einen anderen Begriff als „Auftraggeber" nehmen musste. Im BDSG-alt heißt diese Rolle bis heute noch „Verantwortliche Stelle". Das ist zwar sperriger, birgt aber nicht so leicht das Risiko einer Verwechslung mit dem allgemeinen Begriff eines Verantwortlichen, der ja auch in anderem Zusammenhang genutzt werden kann.

Die oben genannte Begriffsdefinition kann insbesondere dann zu Problemen führen, wenn man den Begriff „Verantwortlicher" einerseits im Sinne der Definition – also als bestimmte Rolle – versteht und andererseits unabhängig davon als denjenigen, der für etwas „verantwortlich" ist. So ist es im Art. 82 „Haftung und Recht auf Schadenersatz" Abs. 3 DS-GVO geschehen. Dort steht:
„Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist."

Jan Philipp Albrecht schreibt dazu in seinem Buch „Das neue Datenschutzrecht" im Kap. 8 Rn. 22:

*„Anders als der verunglückte Wortlaut der deutschen Sprachfassung von Art. 82 Abs. 3 DSGVO nahelegt, kommt es nicht darauf an, dass der Schädiger für die Datenverarbeitung verantwortlich iSv Art. 4 Nr. 7 DSGVO ist, sondern dass ihn **kein Verschulden** an der Datenschutzrechtswidrigen Verarbeitung trifft."*

In der englischen Version besteht dieses Problem zwar nicht, aber sehr sprechend sind die Begriffe für Auftraggeber und Auftragnehmer dort auch nicht. Im englischen Original lauten sie *„controller"* und *„processor"*.

Insbesondere für IT-ler klingt das mehr nach technischen Bauteilen als nach den Rollen, für die sie stehen.

Teil II: Toter Code

Erläuterung

Toter Code ist in der Programmierung ein Begriff für Teile eines Computerprogramms, die an keiner Stelle im Programm verwendet werden.[18]

In der Schreibweise eines Pseudocodes[19] könnte das z. B. folgendermaßen aussehen:

```
wenn x >= 0 dann   z=1
          sonst
                   wenn x=2 dann z=2
                               sonst z=0.
```

Das bedeutet, die Variable „z" soll also den Wert „1" annehmen, wenn die Variable „x" positiv (größer oder gleich 0) ist. Anderenfalls („sonst") soll sie den Wert „0" annehmen, mit der einen Ausnahme, nämlich wenn „x=2" ist. In diesem Fall soll „z=2" sein.

Dieser explizit abgefragte Sonderfall „x=2" wird jedoch an der abgefragten Stelle nie erreicht, denn er steht im „sonst"-Zweig[20] der oberen Abfrage – also dem Fall, bei dem „x >= 0" **nicht erfüllt** und somit die Variable „x" negativ ist. Ein negativer Wert von x kann jedoch niemals „2" sein, sodass bei diesem zweiten „wenn"-Zweig immer der „sonst"-Zweig ausgeführt wird und somit der „dann"-Zweig dieser zweiten Abfrage nie ausgeführt werden kann.

Ähnliches kann es in Gesetzen geben, wenn dort Fälle geregelt werden, die es – zumindest an der Stelle an der sie stehen – nicht geben kann.

6. Beispiel: Absatz mit einer Erweiterung des Anwendungsbereiches, der jedoch in keinem Fall relevant sein kann

§ 32 Abs. 2 BDSG-alt lautet:
„Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden."[21]

§ 27 Abs. 2 BDSG-alt lautet
„Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind."[22]

Die im § 27 Abs. 2 BDSG-alt angegebene Bedingung für die Nutzung (bzw. Nichtnutzung) des Abschnitts[23] beschreibt mit anderen Worten genau den Fall, der im § 32 Abs. 2 BDSG-alt angegeben ist. Dieser Fall kann aber nie eintreten, weil der gesamte Abschnitt 3 in diesem Fall ja nicht gilt und somit auch nicht der darin enthaltene § 32 Abs. 2 BDSG-alt, der die Ausnahme von der Ausnahme darstellen soll.

Vereinfacht ausgedrückt steht im § 32 Abs. 2 BDSG-alt, dass der Absatz 1 auch für Daten in einer unstrukturierten Papierablage gilt und im § 27 Abs. 2 BDSG-alt steht, dass der Abschnitt 3 (und somit auch § 32) für Papierablage nicht gilt.

Auf die hier beschriebene Problematik angesprochen erwiderte ein Jurist dem Autor einmal *„lex specialis derogat legi generali"*[24]. Dieses im Datenschutzrecht oft anzuwendende Prinzip kann in diesem Fall aber – seriös ausgelegt – nicht gelten, weil das „lex specialis" ja gar nicht erst gelesen wird, wenn man das Gesetz für den nicht anwendbaren Fall auch nicht weiterliest. Computer sind in solchen Fällen jedenfalls sehr konsequent.

Das oben beschriebene Problem von § 32 Abs. 2 BDSG-alt tritt übrigens nicht nur mit dem § 27 Abs. 2 BDSG-

alt auf, sondern auch schon mit dem § 1 Abs. 2 Nr. 3 BDSG-alt. Auch dort steht, im „Zweck und Anwendungsbereich des Gesetzes“, dass die Verarbeitung personenbezogener Daten für nichtöffentliche Stellen (Abschnitt 3 mit den §§ 27 bis 38a) nicht für unstrukturierte Papierablage gilt, die laut § 32 Abs. 2 dann aber ausnahmsweise doch relevant sein soll.

Im § 12 (Anwendungsbereich des Abschnitts 2 für die „öffentlichen Stellen“ – bestehend aus den §§ 12 - 26) Abs. 4 BDSG-alt steht:
„Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16, 19 bis 20.“

Der Abschnitt 2 für öffentliche Stellen gilt aber sehr wohl auch für Daten in einer unstrukturierten Papierablage. Das bedeutet, dass in dem in § 12 Abs. 4 BDSG-alt beschriebenen Fall einer Verarbeitung von Beschäftigtendaten der § 32 in einem ganz anderen Kontext zur Anwendung kommt als es im Abschnitt 3 vorgesehen ist. In diesem Fall kann der Absatz 2 des § 32 zwar zur Anwendung kommen, aber er ist nicht nötig und somit redundant. Denn vom Abschnitt 2 kommend gibt es ja die Einschränkung gar nicht, dass die Verarbeitung einer unstrukturierten Papierablage vom Gesetz ausgenommen ist. Auch aus § 1 BDSG-alt gibt es in diesem Fall kein Problem mehr.

Übertragen auf die Informatik entspricht das einem sogenannten „Spaghetticode“[25], bei dem Programme in den Anfängen der Programmierung oft durch viele Sprungbefehle „GOTO“ extrem unübersichtlich wurden und dadurch nicht mehr wartbar waren. Das hatte zur Folge, dass es bei neuen Anforderungen oft günstiger war, die Software neu zu erstellen als die vorhandene noch einmal anzupassen.

Genau das ist ja nun auch mit dem Datenschutzrecht geschehen. Bevor man sich entscheidet, ob es übersichtlicher wurde, sollte man aber die folgenden Beispiele lesen, die sich teilweise bereits auf dieses neue Recht beziehen.

Teil III: Sprachwirrwarr

Erläuterung

Die folgenden Beispiele (7. bis 11. Beispiel) haben gemeinsam, dass sie sprachlich etwas zu bieten haben. Während die beiden nächsten Beispiele einfach nur kurios im Sinne dieses Artikels, aber ansonsten datenschutzrechtlich harmlos sind, betrifft das 9. Beispiel die mehrfache Verneinung, die durchaus verwirren und somit zu Verständnisproblemen führen kann. Die letzten beiden Beispiele können echte Kopfschmerzen bereiten (10. Beispiel) oder zu grundsätzlichen Missverständnissen führen (11. Beispiel).

7. Beispiel: Sehr langer Satz

Die DS-GVO beginnt auf der ersten Seite nach der Überschrift und einem einleitenden Block mit folgendem Satz(-anfang):

„DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,
auf Vorschlag der Europäischen Kommission,
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1]*,*
nach Stellungnahme des Ausschusses der Regionen[2]*,*
gemäß dem ordentlichen Gesetzgebungsverfahren[3]*,“*

Die drei angegebenen Fußnoten stehen dann auch noch auf der 1. Seite, spielen im Zusammenhang mit diesem Beispiel aber keine Rolle und wurden daher hier weggelassen.

Wenn man nun danach sucht, wo dieser offensichtlich nicht abgeschlossene Satz weitergeht, dann kann man lange suchen. Auf den folgenden 106 Seiten werden zunächst die insgesamt 173 Erwägungsgründe der DS-GVO abgedruckt, die ihrerseits aus vielen vollständigen Sätzen – jeweils mit einem Punkt am Ende und oft sogar aus mehreren Absätzen – bestehen.

Aber dann – ganz plötzlich auf Seite 107 – also noch vor dem ersten Artikel der Verordnung geht der Satz wie folgt weiter:

„HABEN FOLGENDE VERORDNUNG ERLASSEN:“

Danach kommen dann die 99 Artikel der Verordnung.

Dieser Satz hat eine faire[26] Chance, in das *„Guinness Buch der Rekorde“*[27] aufgenommen zu werden.

In der Informatik haben sich Programmierrichtlinien sehr bewährt, in denen Regeln stehen, die beim Erstellen von Software einzuhalten sind. Dort steht meistens auch etwas über die Größe eines Moduls, das für Menschen[28] möglichst lesbar bleiben soll. Anderenfalls ist so ein Programm nicht wartbar[29]. Bei deutlich mehr als einer Seite sollte dieser Code möglichst in mehrere überschaubare Teile aufgeteilt[30] werden.

Wenn ein Programmierer einen Code liefern würde, der z. B. eine „IF–THEN–ELSE“-Anweisung enthält, deren „THEN“- oder der „ELSE“-Zweig erst über 100 Seiten später zu Ende ist, dann wäre das ein Grund zur fristlosen Kündigung.[31]

8. Beispiel: Gendering / Geschlechtergerechte Sprache

Manche Datenschützer haben gar nicht mitbekommen, dass sich das BDSG-alt im letzten Jahr geändert hat. Neben ein paar wenigen (wenn auch wichtigen) Veränderungen die BfDI betreffend, hat sich inhaltlich am Gesetz nichts geändert. Es fand jedoch ein „Gendering“[32] statt, bei dem viele Paragrafen in eine „geschlechtergerechte Sprache“[33] überführt wurden.

Der § 23 Abs. 1 Satz 3 BDSG-alt lautet beispielsweise[34]:
„Die Bundespräsidentin oder der Bundespräsident entlässt die Bundesbeauftragte oder den Bundesbeauftragten, wenn diese oder dieser es verlangt oder auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages, wenn Gründe vorliegen, die bei einer Richterin auf Lebenszeit oder einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.“

Man müsste so etwas eigentlich für einen leicht durchschaubaren Aprilscherz

halten, aber so steht es tatsächlich im Gesetz. Der Klarheit, Transparenz oder Übersichtlichkeit dient dieser Trend jedenfalls nicht. Es lässt einem einfach nur die Tränen in die Augen schießen, wenn man sieht, wie die Sprache verhunzt wird. Andererseits macht es aber auch wütend, denn hier ist kein Fehler passiert wie (hoffentlich) bei den anderen Beispielen, sondern diese Veränderung wurde ganz bewusst so herbeigeführt. Dass sich irgendjemand besser oder gerechter behandelt fühlt, wenn Gesetze oder die deutsche Sprache insgesamt so umgeschrieben werden, darf bezweifelt werden.

Selbst wenn sich jemand finden sollte, der sich über solch einen Satz wie oben erfreut, dann müsste man im Sinne einer Abwägung unter Berücksichtigung aller Betroffenen (das ist z. B. jedermann, der das Gesetz lesen, verstehen, interpretieren und Anderen erläutern muss – also mindestens jeder Datenschützer) zu dem Schluss kommen, dass ein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Anpassung dieses Satzes an diese Gesetzesänderung überwiegt.

Ein Lichtblick ist immerhin, dass es Stellen im Gesetz gibt, die nicht angepasst wurden. Paragraf 43 Abs. 3 Satz 2 BDSG-alt blieb beispielsweise unverändert:

„Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen.“

Im BDSG-neu hat man die Schreibweise weitgehend beibehalten. Die Unübersichtlichkeit wird nur dadurch etwas abgeschwächt, dass kürzere Sätze gebildet wurden.

Ein Beispiel hierzu, das dem oben wiedergegebenen Satz nahe kommt, findet sich im § 11 Abs. 1 BDSG-neu:

„Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen. Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst haben.“

Alternativ hierzu enthalten viele Texte auch einen einleitenden Satz mit einer entsprechenden Klarstellung. Der folgende Satz ist einem Text einer Professor**<u>in</u>** der TU Darmstadt entnommen:

„Die Verwendung männlicher Sprache erfolgt im Interesse von Klarheit, Kürze und Einfachheit verbunden mit der Bitte, nicht das grammatische Maskulinum auf das biologische Geschlecht zu reduzieren.“

Danach kann man dann wie gewohnt weiterschreiben, und der Text bleibt lesbar. Wenn man so einen Satz aber jedem Text – einschließlich jedem Gesetz – voranstellen muss, dann stellt das auch eine wenig sinnvolle Redundanz dar. Eventuell kann man den Satz noch einmal leicht modifizieren und an sehr zentraler Stelle einmalig platzieren, wie beispielsweise im BGB oder auch gleich im Grundgesetz.

Zu diesem Beispiel gibt es in der Informatik kein Äquivalent.

9. Beispiel: mehrfache Verneinung

Der Satz aus § 27 Abs. 2 BDSG-alt war auch bereits im 6. Beispiel ein Thema, wird hier aber als Beispiel zu dem Thema „mehrfache Verneinung“ noch einmal herangezogen. Wie man sieht, sind manche Sätze im BDSG-alt sehr ergiebig.

In der Informatik sind doppelte Verneinungen überhaupt kein Problem – sie heben sich einfach auf. Wenn man sagt: „Ich habe nicht kein Geld“ dann bedeutet das, dass man Geld hat. Wenn man eine sechsfache Verneinung hat, dann entspricht das einer dreifachen doppelten Verneinung, sodass sich diese auch alle aufheben. Wenn man eine beliebige gerade Anzahl von Verneinungen hat, dann heben sich diese immer auf. Wenn man eine beliebige ungerade Anzahl von Verneinungen hat, dann entspricht das immer einer einfachen Verneinung.

Sätze mit mehreren Verneinungen werden für den menschlichen Leser sehr schnell kompliziert und schwer verständlich. Darüber hinaus haben Verneinungen umgangssprachlich manchmal eine andere Bedeutung, als nach der strengen Aussagenlogik: Wenn zum Beispiel jemand fragt: „Habe ich nicht recht?“ und man antwortet mit „ja“, dann bedeutet das im Sinne der Aussagenlogik, dass man ihm bestätigt, „nicht recht“ zu haben. Umgangssprachlich wird eher das Gegenteil gemeint sein. Es stellt sich also die Frage, welche Interpretation in solchen Fällen bei Gesetzen zur Anwendung kommen soll.

§ 27 Abs. 2 BDSG-alt lautet

„Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.“

Die Begriffe „automatisierte Datei“ und „nicht automatisierte Datei“ sind im § 46 Abs. 1 BDSG-alt definiert, und da beginnt bereits das Problem. Wenn das eine das Gegenteil des anderen sein soll, wie es die Namen nahelegen, dann bräuchte man dafür keine zwei Definitionen – oder etwa doch?

§ 46 Abs. 1 BDSG-alt lautet:

„Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei
1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).
Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.“

Der Begriff „automatisierte Datei“ besteht aus zwei Worten, und das „nicht“

in „nicht automatisierte Datei" bezieht sich nur auf das erste Wort „automatisiert" und nicht auf den gesamten Begriff, denn die „nicht automatisierte Datei" ist nach der Definition nach wie vor eine Datei, was bei einer reinen Verneinung (dem Gegenteil des Begriffes „automatisierte Datei") nicht so wäre.

Die zwei Definitionen für „automatisierte Datei" und „nicht automatisierte Datei" sind somit nicht das Gegenteil voneinander. Erstere ist eine Computerdatei, letztere z. B. ein Papierordner, dessen Inhalte aber noch nach bestimmten Merkmalen geordnet sind (z. B. nach Alphabet) und entsprechend ausgewertet werden können. Der letzte Satz von § 46 Abs. 1 BDSG-alt steht z. B. für eine unsortierte Papierablage, für die es aber keinen definierten Begriff gibt – leider. Gemeint ist damit das, was im § 27 Abs. 2 BDSG-alt (s. oben) als „außerhalb von nicht automatisierten Dateien" umschrieben wird.

Wenn jedoch mit „nicht automatisierte Datei" z. B. ein Papierordner mit Registern gemeint ist, dann schließt „außerhalb…" davon auch jede Computerdatei mit ein, also auch eine „automatisierte Datei", was aber definitiv nicht gemeint ist.

Im Sinne der reinen Aussagenlogik lässt sich das alles nicht erschließen. Man muss einfach wissen, was mit diesen Begriffen bzw. Formulierungen gemeint ist, und sollte nicht zu sehr über den Wortlaut nachdenken – das hilft nicht, sondern verwirrt nur.

Das bisher zu § 27 Abs. 2 BDSG-alt Dargestellte ist bereits verwirrend genug, aber es kommt noch ein Aspekt hinzu, der sogar eine weitere Kategorie der hier aufgezählten Kuriositäten darstellen könnte: Es handelt sich bei diesem Absatz nämlich auch um ein Beispiel für eine Kombination aus „Selbstbezogenheit", „Widersprüchlichkeit" und „Zirkelhaftigkeit" – alles wichtige Bestandteile eines Paradoxons.[35]

Einfache Beispielsätze hierzu sind:

- „Keine Regel ohne Ausnahme." (Der Satz selbst ist auch eine Regel.)
- „Dieser Satz enthelt drei Feler." (Zwei Schreibfehler und die Aussage des Satzes.)
- Pinocchio sagt: „Meine Nase wächst gerade." (Überliefert ist, dass seine Nase wächst, wenn er lügt.)

Die Aussage im § 27 Abs. 2 BDSG-alt *„Die Vorschriften dieses Abschnittes gelten nicht für…"* beziehen sich auf den gesamten Abschnitt 3 BDSG-alt, bestehend aus den Paragrafen 27 bis 38a. Der § 27 ist selbst Teil dieses Abschnitts 3 und gilt somit unter der angegebenen Voraussetzung nicht. Wenn der § 27 aber nicht gilt, dann entfällt auch die Einschränkung von Absatz 2, wonach er nicht gilt ➔ also gilt er doch usw.

In der Informatik kennt man so etwas leider auch. Das ist der Punkt, an dem man seinen Computer aus- und wieder einschaltet.

10. Beispiel: Verarbeitung besonderer Kategorien personenbezogener Daten

Die „Verarbeitung besonderer Kategorien personenbezogener Daten" ist in Art. 9 DS-GVO geregelt. Der Artikel ist bereits recht umfangreich, aber für sich genommen noch verständlich. Er enthält (wie andere Artikel auch) jedoch Öffnungsklauseln bzw. Konkretisierungsvorgaben, sodass die nationalen Gesetzgeber sich hierzu auch auslassen dürfen. Das Ergebnis ist im § 22 BDSG-neu nachzulesen.

Eine verworrenere rechtliche Vorgabe kann man sich nicht mehr vorstellen.[36] Was das Zusammenspiel dieser beiden Rechtsgrundlagen genau bedeutet, kann hier nicht wiedergegeben werden – es würde den Rahmen dieses Beitrags sprengen. Wer sich damit befassen möchte bzw. muss, dem sei ein sechsseitiger Artikel von Thilo Weichert in der DuD[37] empfohlen, der sich ausschließlich mit diesem Thema befasst.

Ein kleiner Auszug daraus:
„…§ 22 BDSG-neu regelt minimalistisch die Verarbeitung ‚besonderer Kategorien personenbezogener Daten', indem er in Abs. 1 den Inhalt der Öffnungsklauseln in Art. 9 Abs. 2 DS-GVO teilweise fast wortgetreu wiederholt: Aus lit. b DS-GVO wird Nr. 1 lit. a BDSG-neu; aus lit. h DS-GVO wird Nr. 1 lit. b BDSG-neu; aus lit. i DS-GVO wird Nr. 1 lit. c; aus lit. g DS-GVO wird Nr. 2 lit. a-d BDSG-neu, wobei normative Begrenzungen darin liegen, dass nur öffentliche Stellen berechtigt werden und dass eine Güterabwägung zur Pflicht gemacht wird…."

Im Fazit steht dann:
„…Derweil bleibt den Anwendern und Betroffenen nichts anderes übrig, als zu versuchen, trotz des Regelungschaosses effektiven Grundrechtsschutz zu realisieren…"

Eventuell hilft Erwägungsgrund 58 Satz 1 DS-GVO an dieser Stelle weiter:
„Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden."

Sollte das dann nicht auch für das BDSG-neu gelten, das ja die Öffnungsklauseln der DS-GVO nur umsetzt und sich somit auch selbst an deren Vorgaben zu halten hat?

Wie viele Datenschützer, egal ob Juristen oder Informatiker, das Zusammenspiel[38] von Art. 9 DS-GVO und § 22 BDSG-neu verstehen und den Mitarbeitern der betreuten Unternehmen verständlich erläutern können, ist nicht abzusehen. Wie kann man als Datenschützer darauf überhaupt reagieren?

Im Mittelalter gab es Bräuche[39], die man gegenüber den ausgemachten Verantwortlichen für ein Unheil, das diese der Allgemeinheit zugefügt hatten, für angemessen hielt. Beim Sinnieren darüber fällt einem dann aber ein, dass man sich als Datenschützer ja für die Einhaltung der Grundrechte einsetzt, sodass man solche Gedanken sofort wieder verwerfen muss.

Aber: Die Gedanken sind frei, und sie kommen immer wieder.

11. Beispiel: Korrekte Deutung einer Verschachtelung

Artikel 39 „Aufgaben des Datenschutzbeauftragten" Abs. 1 DS-GVO beginnt mit:
„Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:"

Nach einem Absatz zu lit a) kommt dann folgender Absatz zu lit b):
„Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitglied-

staaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;"

Der Autor dieses DANA-Artikels[40] las vor einigen Monaten in einem Buch[41] über die Umsetzung der DS-GVO in Unternehmen folgenden Satz:
„Ferner fordert Art. 39 Abs. 1 lit (b) DSGVO ausdrücklich die ‚Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter' durch den Datenschutzbeauftragten."

Der Satz klingt zunächst unspektakulär. Schließlich gehörte die Schulung auch bisher zu den Aufgaben eines DSB (§ 4g Abs. 1 Nr. 2 BDSG-alt) und warum sollte das mit der DS-GVO anders sein.

Es stellt sich aber die Frage, ob Art. 39 Abs. 1 lit b) DS-GVO tatsächlich diese Anforderung enthält.

Bevor diese Frage beantwortet wird, soll hier gezeigt werden, mit welchem Hilfsmittel man sich in der Informatik die Übersicht über Verschachtelungen erhält: Texte werden mit jeder Schachtelungstiefe immer weiter eingerückt.[42]

Folgender Satz kann durch Einrückungen deutlich an Übersichtlichkeit gewinnen:
„Denken Sie, wie tragisch der Krieger, der die Botschaft, die den Sieg, den die Athener bei Marathon, obwohl sie in der Minderheit waren, nach Athen, das in großer Sorge, ob es die Perser nicht zerstören würden, schwebte, erfochten hatten, verkündete, brachte, starb."

```
Denken Sie,
    wie tragisch der Krieger,
        der die Botschaft,
            die den Sieg,
                den die Athener bei Marathon,
                    obwohl sie in der Minderheit waren,
        nach Athen,
                        das in großer Sorge,
                            ob es die Perser nicht zerstören würden,
                        schwebte,
                erfochten hatten,
            verkündete,
        brachte,
    starb.
```

Grafik: Verschachtelter Satz –
durch Einrückungen verständlich(er) dargestellt.

Einrückungen sind zwar mit Sicherheit keine Erfindung aus dem Bereich der Informatik, aber beim Programmieren wird davon konsequent Gebrauch gemacht. Von Weitem betrachtet sehen ausgedruckte Computerprogramme manchmal tatsächlich so schlangenlinienförmig aus wie in der Grafik dargestellt.

Art. 39 Abs. 1 lit b) DS-GVO ist zwar nicht annähernd so tief verschachtelt aber mit den richtigen Einrückungen wird er trotzdem deutlich klarer:
„Überwachung der Einhaltung
- *dieser Verordnung,*
- *anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten,*
- *der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und*
- *der diesbezüglichen Überprüfungen;"*

Über allen Aufzählungspunkten steht also „Überwachung der Einhaltung". Die dann folgenden Aufzählungspunkte gehören somit nicht zu den Aufgaben eines DSB, sondern nur die „Überwachung der Einhaltung" dieser Punkte.

Der Autor des o.g. Buches über die Umsetzung der DS-GVO antwortete dem Autor dieses DANA-Artikels, dass er den Satz bisher anders gelesen hatte:
„Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich
- *der Zuweisung von Zuständigkeiten,*
- *der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und*
- *der diesbezüglichen Überprüfungen;"*

Der Buchautor ergänzte jedoch, dass er sich nun der anderen Interpretation des Satzes anschließen und dies in neueren Auflagen des Buches auch berücksichtigen würde.

Der Punkt, um den es hier geht, ist nicht, ob es zu den Aufgaben eines DSB gehört, auch Schulungen durchzuführen. Darauf wird es in der Praxis wohl sowieso meistens hinaus laufen – egal, ob dies formal zu dessen Aufgaben gehört oder nicht. Der entscheidende Punkt ist, dass bei der alternativen Auslegung des Satzes auch die „Zuweisung von Zuständigkeiten" zu den Aufgaben eines DSB gehören würde. Das wäre jedoch ein vollkommen neues Verständnis der Rolle und der Stellung eines DSB, wovon in der öffentlichen Diskussion bisher nichts zu hören war.

Trotzdem scheint die alternative Interpretation dieses Satzes recht verbreitet zu sein. Der DANA-Autor konnte jedenfalls schon mehrere Datenschützer von seiner Interpretation überzeugen, nachdem diese zuvor von der alternativen (zweiten) Variante fest überzeugt waren.

Auch die Info 6[43] der BfDI „Datenschutz-Grundverordnung" enthält auf Seite 25 eine nicht eindeutige Aufzählung der Aufgaben:
„Art. 39 DSGVO normiert die vom Datenschutzbeauftragten wahrzunehmenden Aufgaben – wie Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters sowie der Beschäftigten, Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften, Schulungen und Zusammenarbeit mit der Aufsichtsbehörde."

Teil IV: Fazit

Gesetze sind auch nur Software.

1 Im bis 25. Mai 2018 noch gültgen BDSG (im folgenden Text „BDSG-alt") heißt es „Bestellung", in der Datenschutzgrundverordnung und im BDSG neue Fassung (im folgenden Text „BDSG-neu") heißt es „Benennung".

2 Siehe hierzu auch das „Berufliche Leitbild der Datenschutzbeaufragten" des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

3 Er ist bestellter Stellvertreter des Konzerndatenschutzbeaufragten eines deutschen Unternehmens.

4 Diese Diskussionspartner waren häufig auch Juristen, die sich auf den Datenschutz spezialisiert haben.

5 Siehe hierzu speziell das elfte der folgenden Beispiele.

6 Zum Beispiel, indem Konstrukte wie „GOTO" oder undefinierte Variablen in

manchen Programmiersprachen nicht vorhanden/erlaubt sind. Erläuterungen dazu kommen in den folgenden Beispielen.

7 Es handelt sich hier um die sogenannte „herrschende Meinung“ – siehe: https://de.wikipedia.org/wiki/Herrschende_Meinung

8 So sehen es jedenfalls die DS-Aufsichtsbehörden, und so beschreibt es auch Jan Philipp Albrecht in seinem Buch „Das neue Datenschutzrecht der EU“ Teil 3 Rn. 5 und Teil 5 Rn. 22. Die Argumentation dort ist jedoch auch etwas konstruiert.

9 Hier wird bewusst auf den Begriff „übermitteln“ verzichtet, weil es sich bei einer ADV gerade nicht um „Übermittlung“ von Daten handelt, wie im folgenden Text erläutert wird.

10 Die Schweiz ist nicht Mitglied der EU und auch nicht des Europäischen Wirtschafsraums (EWR), aber sie ist anerkanntermaßen ein sicheres Drittland mit einem angemessenen Datenschutzniveau.

11 Das gilt unabhängig von allen Vorkehrungen zum Schutz der personenbezogenen Daten wie Standardvertragsklauseln, EU-US Privacy Shield oder verbindlichen Unternehmensregelungen.

12 Siehe: https://de.wikipedia.org/wiki/Kopplung_(Softwareentwicklung)

13 Siehe: https://de.wikipedia.org/wiki/Koh%C3%A4sion_(Informatik)

14 So kann man es in vielen Fachartikeln und Büchern nachlesen, und auch Vertreter von Aufsichtsbehörden haben diese Sichtweise bereits vertreten.

15 Teilweise wird auch argumentiert, dass „Treu und Glauben“ nicht im Sinne des BGB zu interpretieren ist, sondern als „Angemessenheit im Sinne eines Ausschlusses unverhältnismäßiger Verarbeitungen“. Das mag sein, ändert aber nichts daran, dass in der deutschen Übersetzung „Treu und Glauben“ steht und nicht z. B. „Angemessenheit“ oder „Verhältnismäßigkeit“ oder einfach nur „Fairness“.

16 Es sind die Paragrafen: 157, 162, 242, 257, 307, 320 und 815.

17 Bzw. „Aufragsverarbeitung“ (AV) – wie es jetzt in der DS-GVO genannt wird.

18 Siehe: https://de.wikipedia.org/wiki/Toter_Code

19 Siehe: https://de.wikipedia.org/wiki/Pseudocode

20 Typisch sind in Programmiersprachen die englischen Begriffe wie „if“, „then“ und „else“ statt „wenn“, „dann“ und „sonst“, was inhaltlich jedoch nichts ändert.

21 Vereinfacht ausgedrückt steht dort, dass Absatz 1 immer anzuwenden ist – egal ob die Daten automatisiert oder z. B. in Papierform vorliegen.

22 Dieser Satz aus § 27 Abs. 2 BDSG-alt bietet über das hier Beschriebene hinaus noch mehr Stoff – siehe dazu Beispiel 8.

23 Es handelt sich um Abschnitt 3 „Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen“ bestehend aus den §§ 27 bis 38a.

24 Das besondere Gesetz verdrängt das allgemeine Gesetz. Siehe https://de.wikipedia.org/wiki/Lex_specialis

25 Siehe: https://de.wikipedia.org/wiki/Spaghetticode

26 Die möglicherweise korrektere Schreibweise: „…eine nach Treu und Glauben angemessene Chance…“

27 Siehe: https://de.wikipedia.org/wiki/Guinness-Buch_der_Rekorde

28 Die Computer hätten mit mehreren hundert Seiten kein Problem.

29 Siehe 6. Beispiel.

30 Das Prinzip wird auch in der Informatik als „divide and conquer“ bzw. „teile und herrsche“ bezeichnet – siehe: https://de.wikipedia.org/wiki/Teile_und_herrsche_(Informatik)

31 Wenn der zuständige Richter des Arbeitsgerichts zufällig auch eine Informatikausbildung hätte, käme das Unternehmen mit der Kündigung auch durch.

32 Siehe: https://de.wikipedia.org/wiki/Gendering

33 Siehe: https://de.wikipedia.org/wiki/Geschlechtergerechte_Sprache

34 Die danach folgenden Absätze und auch die Paragrafen vor oder nach dem § 23 BDSG-alt sind ähnlich formuliert.

35 Siehe: „Die Scheinwelt des Paradoxons“, von Patrick Hughes und George Brecht, Vieweg Verlag, ISBN 3 528 083794

36 Vorstellen kann man sich auch die hier beschriebene nicht.

37 DuD Datenschutz und Datensicherheit, Heft 9/2017, Artikel von Thilo Weichert: „‚Sensitive Daten‘ revisited“

38 Zu bedenken ist auch, dass der Art. 9 DS-GVO trotzdem gültg bleibt. Der § 22 BDSG-neu wirkt nur im Rahmen der Öffnungsklauseln.

39 Neben der Prügelstrafe, die heute auf größeren Widerstand stoßen würde, gab es auch das mildere Mittel des Teerens und Federns. Bedenken dagegen gäbe es zwar sicher auch, aber eventuell käme eine Mehrheit zu dem Schluss, dass die Wiedereinführung dieses Brauches besser wäre als gar nichts zu unternehmen.

40 Die Erwähnung von „DANA“ ist hier wichtig, denn um den Autor des Artikels 39 handelt es sich hier nicht.

41 Titel: „EU-Datenschutz-Grundverordnung im Unternehmen“, Autor: Tim Wybitul, Kap. IV, Rn. 343.

42 Siehe auch die Erläuterung zu „Toter Code“ vor dem 6. Beispiel.

43 Siehe: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?

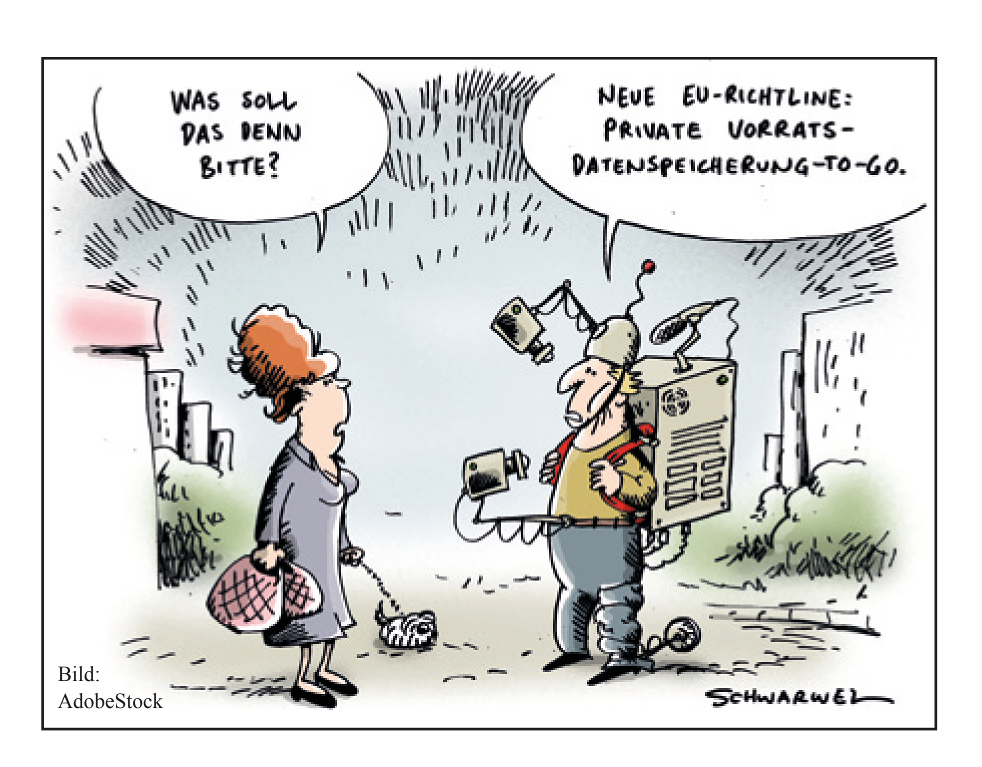


Bild: AdobeStock

Ute Bernhardt

Wenn aus Spiel Wirklichkeit wird

Potenziale kollaborativer Augmented Reality



Pokémon – Bild: ClipDealer

Virtuelle und „erweiterte Realität" – Virtual und Augmented Reality – mit Smartphones ist heute Alltag. Mit diversen Datenbrillen sollen neue Anwendungen auf dem Markt etabliert werden. Diese Entwicklung erfordert es, sich mit den Potenzialen ihres kollaborativen Einsatzes näher zu beschäftigen. Welche Konsequenzen hat ihr Einsatz durch kriminelle Gruppen oder Terroristen für die zivile Sicherheit?[1]

Augmented Reality auf dem Weg zum Massenmarkt

Die um digitale Informationen *„erweiterte Realität" – Augmented Reality, kurz: AR* – ist mittlerweile zu einem Massenmarkt mit Millionen Endkunden geworden. Die Palette der AR-Brillen wächst ebenso kontinuierlich wie deren Leistungsfähigkeit. Mit *Pokémon Go* war 2016 ein Computerspiel erfolgreich, bei dem Smartphones als AR-Werkzeug dienen, um Spielfiguren in einer realen Umgebung aufzufinden. Bei derartigen AR-Spielen, perspektivisch aber vor allem für betriebliche Anwendungen liefern Datenbrillen eine möglichst realistische Kombination von Umgebungsbild und virtuellen Daten und lassen die Hände frei für Bedienaufgaben. Für solche Datenbrillen gibt es bereits neben Einzel- auch AR-Gruppenspiele wie etwa *„Life is Crime"*, die daraus bestehen, in der eigenen realen Umgebung bei einer virtuellen kriminellen Gang aktiv mitzuwirken als – so die Werbung – Weg, um das „Leben eines Kriminellen zu führen, ohne dafür ins Gefängnis zu müssen"[2]. Die deutsche Innenministerkonferenz hat beschlossen, Datenbrillen zu evaluieren. Insgesamt wurden für Datenbrillen schon viele Anwendungsideen entwickelt, einige davon gehen deutlich über Computerspiele und Unterhaltung hinaus. So erprobt Volkswagen den Einsatz von Datenbrillen in der Logistik.[3]

Schon bei Google Glass als erster breit beworbener vernetzten Datenbrille für Endkunden wurde bereits vor einigen Jahren eine Datenschutzdebatte angestoßen. Die Ausstattung mit Videokamera, Mikrofon und der Möglichkeit sofortiger akustischer oder optischer Rückmeldungen, die in das Sehfeld projiziert werden, war diese Debatte konzentriert auf die durch unbemerkte und allgegenwärtige Aufzeichnung und Übermittlung von Live-Videos der Umgebung des Brillenträgers geschaffenen Möglichkeiten zur individualisierten Videoüberwachung der vom Nutzer beobachteten Personen, dem Verlust von Kontrolle und Vertraulichkeit und durch die Speicherung und Analyse der Daten auf zentralen Servern zur weitergehenden Analyse der Daten und den damit drohenden Verlust von Autonomie und Reputation[4].

Diese auf den Datenschutz bezogene Diskussion kreist bisher darum, Datenbrillen als vernetzte Einzelsysteme[5] und das Verhältnis einzelner Nutzer zu ihren Gegenübern zu betrachten. Deutlich gravierender können die Folgen sein, wenn eine Gruppe von Personen AR-Brillen nutzt. Die Betrachtung von Datenbrillen als Kollaborations- und Gruppenunterstützungssysteme, die daraus folgenden Potenziale und deren Folgen fand bisher jedoch kaum statt. In diesem Beitrag sollen daher spezifische Möglichkeiten und Konsequenzen eines Einsatzes durch Gruppen von kollaborierenden Nutzern betrachtet werden. Ausgangspunkt der weiteren Betrachtung sollen nach einer kurzen Darstellung der Eigenschaften eine Beschreibung bereits dokumentierter Manipulationen der Systeme und die von den Herstellern nicht intendierten oder gar in Abrede gestellten Eigenschaften sein. Dies wird in Bezug gesetzt zu den Zielen bei der ursprünglichen Entwicklung von Datenbrillen und schließlich werden die möglichen Folgen dieser dokumentierten Eigenschaften betrachtet.

Datenbrillen und ihre Eigenschaften

Die zahlreichen Typen von zu irgendeiner Zeit angekündigten[6] oder erhältlichen[7] Datenbrillen machen es wenig sinnvoll, ein einzelnes spezifisches System als Basis einer Analyse auszuwählen. Um als Augmented Reality-Werkzeug eingesetzt werden zu können, müssen alle Geräte Daten aus dem situativen Kontext des Benutzers in dessen Sichtlinie auf ein *head-mounted display* (HMD) projizieren. Üblich ist ein semi-transparentes Brillenglas, patentiert ist bereits eine Kontaktlinse[8]. Um die Umwelt zu erfassen, verfügen sie über Kamera, zumeist auch Mikrofon und Kopfhörer, sowie zunehmend auch über die Fähigkeit, mit mehreren Kameras 3D-Tiefendaten zu ermitteln. Die aktuelle Version der Microsoft Hololens beispielsweise verfügt dazu über sechs Kameras. Die Videodaten werden mit Bildanalyse-Software auf spezifische optische Marker hin analysiert. Es gibt auch Bilderkennungs-Werkzeuge, die eine Gesichtserkennung leisten oder Personen anhand von spezifischen Zusatzmerkmalen erkennen.[9] Für all dies verfügen Datenbrillen über eine mehr oder minder ausreichende Rechenkapazität und Netzwerkanbindung.[10] Verschiedene Systeme sind darauf ausgelegt, zusätzliche Sensoren einzubinden und zu vernetzen, wofür Programmschnittstellen offengelegt werden, die es Entwicklern erlauben, die Datenbrille auf ihre eigene Weise zu nutzen.

Jeder Träger einer Datenbrille erstellt also in aller Regel Audio- und Videoaufnahmen der Umgebung, die der Kommunikation und Interaktion mit Backend-Systemen oder Support-Fachleuten dienen und dazu in Echtzeit an ein Rechenzentrum übermittelt werden, wo die Bilder analysiert und zur Unterstützung oder Aufzeichnung genutzt werden. Wer die Bild- und Tonaufnahmen der Lebensumwelt des Trägers einer Datenbrille sieht, ist dessen Umgebung ebenso unklar wie die Dauer einer Aufzeichnung und die Art der darauf durchgeführten Datenanalyse.

Recht typisch sind die Ziele des versuchsweisen Einsatzes von AR-Brillen bei Kabinenpersonal der Air New Zealand, um spezifische Daten sowie auf Basis einer Analyse von Gesichtszügen den emotionalen Status der einzelner Passagiere einzublenden[11]. Die Datenschutzprobleme dieser intensiven Umgebungsüberwachung sind unmittelbar einsichtig und bereits intensiv diskutiert. Aus Datenschutzsicht lassen sich dabei vor allem die auf Handhabungsaufgaben bezogenen Systeme in betrieblichen Anwendungen noch relativ gut fassen, wenn personenbezogene Daten zwar über die Handlungen der beteiligten Personen erhoben werden, selten aber über unbeteiligte Dritte[12].

Intendierte und nicht-intendierte Nutzung

Für viele der nachfolgend beschriebenen Möglichkeiten gibt es noch keine App zu kaufen. Nötig sind daher gewisse Fertigkeiten in der Programmierung von derartigen oder vergleichbaren Geräten. Einige der beschriebenen Funktionen wurden immerhin bereits in Forschungsprojekten realisiert. Bei der Bewertung des Anpassungsaufwands liefert Google Glass recht gute Vergleichsangaben.

Um offenbar erwartete, von Google nicht gewollte Anwendungen von Google Glass zu verhindern oder zumindest zu ahnden, sah Google in den Nutzungsbedingungen vor, dass das Unternehmen „sofern ein Google Gerät die Entwickler-Regelungen oder andere Übereinkünfte, Gesetze, Regularien oder Policies verletzt", dieses „Glass-Gerät fernabschalten oder das Gerät aus seinen Servicesystemen entfernen kann".[13] Zu Kontrollzwecken und zur Umsetzung dieser Nutzungsbedingung hatte sich Google zudem das Recht vorbehalten, die Ortungsdaten des Nutzers sowie alle aufgenommenen Fotos, Videos und in das Display des Nutzers eingespielte Daten aufzuzeichnen und zu speichern.[14] Damit ist Google in der Position, auf Anforderung oder eigene Initiative alle Daten auf unzulässige Handlungen zu scannen. In Googles Version war Google Glass damit als die zivile Version eines mächtigen Kommando- und Kontroll-Systems angelegt.

Wie viele andere Datenbrillen arbeitet Google Glass mit dem Android Betriebssystem und wurde mit Hilfe gängiger Werkzeuge schon wenige Tage nach Ausgabe der ersten Prototypen an Entwickler *gehackt.* Sie hatten danach vollen Zugang zu allen Komponenten des Systems.[15] Google selbst wollte keine Gesichtserkennungs-Software auf den Markt bringen. Dafür kamen Apps alternativer Anbieter in Umlauf, deren Installation teilweise das Hacken der Google-Datenbrille voraussetze.[16] Googles Überwachungs-Werkzeuge ließen sich damit umgehen.

Solche Sicherheitsprobleme sind nicht spezifisch für Google Glass, da alle Datenbrillen nur eine begrenzte Rechenkapazität haben. Die Microsoft Hololens etwa arbeitet mit dem Betriebssystem Windows 10 und kann mit Hilfe der dafür gefundenen Sicherheitslücken manipuliert werden. Bislang hat kein System mit vergleichbaren Ressourcen gezielten Angriffen dauerhaft widerstehen können. Es ist aller Erfahrung nach also davon auszugehen, dass jedes Datenbrillen-System für Endkunden nach überschaubarer Zeit kompromittiert wird und seine Technik nach Belieben manipuliert werden kann.

Kollaborative Datenbrillen-Systeme und ihre Urspünge

Über die bisher diskutierten Szenarien hinaus gehen Anwendungsfelder, bei denen es um die Interaktion mit Dritten geht, deren Verhalten mit Datenbrillen beobachtet wird[17]. Noch weiter gehen die Konsequenzen, wenn Datenbrillen als Mittel der Gruppenkoordination gegen unbeteiligte Dritte eingesetzt werden, wie es Google schon zu Beginn in seiner Werbung für Google Glass skizziert hat[18]. Extreme dieser Möglichkeiten sind ein Google Glass *ego-shooter*[19] und vergleichbare Produkte wie „RoboRaid" für die Microsoft Hololens[20]. Sie repräsentieren zugleich eine Rückkehr der Datenbrillen zu den historischen Ursprüngen aller AR-Systeme mit HMD, auf die im Folgenden kurz eingegangen werden soll.

Die U.S. Army führte 1993 verschiedene Manöver mit Bodentruppen durch, um neu entwickelte Informations- und Kommunikationstechnik im Einsatz zu erproben. In der so genannten *„Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD)"* überfiel eine sehr kleine Gruppe von Soldaten erfolgreich eine weit größere Einheit und eroberte verschie-

dene Positionen im offenen Feld ebenso wie im Häuserkampf. Unter herkömmlichen militärischen Bedingungen und gleichwertiger Ausstattung wird davon ausgegangen, dass ein erfolgreicherer Angreifer die dreifache Personalstärke benötigt als der Verteidiger. Die Vorläufer von Datenbrillen stellten dieses Verhältnis auf den Kopf: Der unterlegene Verteidiger war dreimal stärker als der Angreifer.

Möglich machten dieses umgekehrte Kräfteverhältnis nicht Techniken wie die einzeln schon lange genutzten Laser- und Infrarot-Sensoren sowie Audio-Verstärkung und Richtmikrofone. Entscheidend war die Vernetzung von Soldaten und Sensoren in einem kollaborativen AR-System. Die Angreifer konnten durch den Sensor-Datenaustausch die Gegner mit passiver Datenerhebung triangulieren und auf einer gemeinsamen Gefechtsfeldkarte markieren. Diese Karte wurde mit anderen Daten in die Displays eingespielt. Mit vernetzten Videokameras wurde unbemerkt um die Ecke gespäht und die Bilder an alle Gruppenmitglieder übertragen. Vor dem Überfall lieferten die Daten in den AR-Displays einen vollständigen Überblick über den Gegner und unterstützten einen hoch koordinierten Ablauf. Die gleichzeitige Datenübermittlung an einen zentralen Befehlshaber erlaubte es, die Aktion in Echtzeit zu verfolgen und mit zusätzlichen Informationen zu unterstützen.[21]

Die umfassende Vernetzung zwischen Soldaten und Kommandeuren erwies sich als äußerst wirksamer *„Force Multiplier“*. Aus den bis in die 1980er Jahre zurück reichenden Ursprüngen[22] wurde ein technologisches Entwicklungs- und Einsatzziel verschiedener Armeen, allen voran der USA.[23] Sie bauten mit einem einheitlichen Kommunikationssystem einen Datenverbund auf[24], mit dem Audio- und Videodaten in Echtzeit zwischen Kampfeinheiten und Kommandozentralen austauscht werden[25]. Die Bilder aus dem Lagezentrum in Weißen Haus bei der Erstürmung des Verstecks von Osama bin Laden in Pakistan zeigten den Einsatz vernetzter Spezialeinheiten und deren Steuerung.

Der Schritt zur alltäglichen militärischen Nutzung von Datenbrillen steht allerdings noch aus; die Systeme sind noch nicht leistungsfähig, robust und genau genug. Derzeit werden diverse Systeme von verschieden Armeen erprobt.[26] So ist die Bundeswehr von der Konzeptionsphase im Programm „Infanterist der Zukunft“[27] mittlerweile zur Kampferprobung übergegangen. Das *Gladius*-System für AR-Anwendungen mit einem HMD wurde 2013 an das Heer für den Einsatz in Afghanistan ausgeliefert.[28] Die Einsätze sind jedoch auf spezielle Aktionen *von Spezialeinheiten oder Geheimdiensten* beschränkt.[29] Trotz dieser Einschränkungen wurde der Markt für AR-Systeme in Kampfeinsätzen auf 8,2 Mrd. Dollar für 2016 geschätzt.[30]

Von der militärischen zur zivilen Nutzung

Nach der Einführung von Google Glass interessierten sich 2014 die Polizeibehörden New Yorks[31] und Dubais[32] für die Nutzungspotenziale. Berichte über Ergebnisse liegen nicht vor. In Deutschland beschäftigte sich die Innenministerkonferenz im Juni 2016 damit, „aus Streifenbeamten vernetzte Polizisten“ zu machen und „Datenbrillen, um Fahndungsfotos oder Einsatzbefehle direkt an jeden einzelnen Polizisten zu verschicken, schon bald zur Standardausrüstung der Beamten“ zu machen.[33]

Was ist nun zu erwarten, wenn Datenbrillen außerhalb von militärischen Kampfzonen im Zivilleben eingesetzt werden? Und – bisher kaum beachtet – was geschieht, wenn Datenbrillen bei kriminellen oder terroristischen Aktivitäten Verwendung finden? Drei einfache Beispiele mit anwachsendem Gefahrenpotenzial sollen dazu dienen, diese Möglichkeiten auszuloten.

Alle beschriebenen Eigenschaften von kollaborierenden Datenbrillen-Systemen sind zum Teil bereits im Rahmen heutiger Systeme verfügbar oder so in Reichweite, dass es nicht mehr als eines Jahres bedürfte, sie zu entwickeln. Noch sind solche Anwendungen aber nicht bekannt. Damit stellt sich im Anschluss die Frage, welche Bedingungen, Szenarien und Interessen für eine solche Nutzung ausschlaggebend sein könnten.

Überwachung und Verfolgung

Eine einfache und vielfach für AR-Brillen gezeigte kollaborative Anwendung ist die Navigation. Wenn eine Navigation per Karte nicht zum Ziel führt, wird ein Nutzer von einer anderen, ortskundigen Person anhand der Videoaufnahmen der Datenbrille zum Ziel gelenkt – entweder durch gesprochene Richtungsangaben oder durch eingespiegelte Richtungspfeile. Ersetzt man nun ein geografisches Ziel mit einer Person, die im Sichtfeld der Datenbrille – möglicherweise automatisch – erkannt, getaggt und hervorgehoben wird, so ist unmittelbar ersichtlich, dass vernetzte Datenbrillen ein erhebliches Potenzial zur Erleichterung bei der Verfolgung von Personen auch in sehr belebter Umgebung haben.

Erweitert man im nächsten Schritt einen solchen einfachen Datenaustausch um die bereits in den 1990er Jahren erprobten Mittel zur Distanzmessung und die passive Triangulation durch zwei und mehr kollaborierende Nutzer von AR-Systemen und ergänzt das durch die mit heutiger Technik mögliche automatische Erkennung und Markierung charakteristischer Features eines Verfolgten aus Videodaten, so sind erhebliche Erleichterungen bei der Verfolgung zu erzielen. Dass die Kommunikationsunterstützung bei Datenbrillen so unauffällig wie möglich gestaltet ist, vereinfacht die Koordination der Verfolger und verringert die Gefahr, dass Gruppen heimlicher Beobachter erkannt werden.

Mit einer weiteren Sensorintegration lässt sich die Leistung eines AR-Systems noch steigern. In Militärmanövern wurde schon gezeigt, dass sich beliebige Sensoren mit AR-Systemen koppeln lassen. Videokameras ließen sich ersetzen oder ergänzen durch Infrarot- und Nachtsicht-Systeme. Das ist eine attraktive Eigenschaft für diverse Outdoor-Spiele. Zugleich ließe sich aber auf diese Weise die von den Sicherheitsbehörden genannte Zahl von bis zu 35 Beamten für eine Observation[34] mit weit weniger Personal durchführen. Auf gleiche Weise könnten aber kriminelle oder terroristische Gruppen ein Opfer verfolgen.

Nach Terroranschlägen mit polizeilich bekannten Tätern wurde in Deutschland und in Frankreich darüber debattiert, dass eine Observation durch Sicherheitsbehörden so viele Ressourcen bindet, dass sie nur in ausgesuchten und dringenden Fällen infrage kommt. Der

ausufernde Einsatz „stiller SMS“ zur Ermittlung des Standorts von Verdächtigen[35] dokumentiert ein hohes Interesse am Einsatz technischer Hilfsmittel. Datenbrillen können den Aufwand für eine Observation eindeutig reduzieren. Noch einfacher wird es, wenn Umgebungsintelligenz in Form von Videokameras für die Personenerkennung oder mobiler „*IMSI-Catcher“*[36] es erlaubt, Daten mit Observationsteams austauschen, die über Datenbrillen verfügen – wie schon in Militärmanövern in den 1990er Jahren beschrieben. Diverse Analysen von Personenflüssen bei Großveranstaltungen[37] auch anhand von Handy-Kennungen zeigen die enormen Potenziale: Auch in großen Menschenmengen lässt sich mit der richtigen Technik zuverlässig observieren. Entsprechende AR-Technologie dürfte daher mit hoher Wahrscheinlichkeit in die Anforderungen an Entwicklung und Beschaffung von Technik für die Sicherheitsbehörden in den nächsten Jahren einfließen.

Wenn eine Observation von Einzelpersonen nicht länger einen derart hohen Personaleinsatz erforderlich macht und da die Technologie heute bereits verfügbar ist, um eine begrenzte Zahl von Personen für unterschiedliche Bedarfe parallel in einer Umgebung zu verfolgen, können Oberservationstechniken von einer Einzelbeobachtung zu einem System der Zonen-Observation gegenüber definierten Personen umgebaut werden. Eine deutlich kleinere Zahl von Sicherheitskräften mit Datenbrillen und Sensoren könnte in einer Zone mehrere markierte Verdächtige zugleich observieren, das über verschiedene Zonen hinweg durchführen und dabei aufgenommenes Videomaterial als Beweismittel nutzen.

Der polizeiliche Nutzen einer solchen Observation lässt sich bereits einfach erkennen an der Observation einer Gruppe von Taschendieben. Die Taschendiebe hätten allerdings denselben Nutzen, wenn sie gemeinsam mit AR-Hilfe auf Beutejagd gehen.

Diebstahl und Einbruch

Auf dieselbe Weise lassen sich Werkzeuge zum Orten und Anzeigen von WLAN-Emittern, Smartphones oder anderen funkgestützten Systemen einbinden, wofür je nach Emitter-Typ Modifikationen der heute in Smartphones vorhandenen Ortungswerkzeuge gegen Diebstahl ausreichen. Bisweilen können komplexere Zusatzinstallationen[38] erforderlich sein.

Mit derselben Kombination von Sensoren können auch Einbrecher WLAN-Emitter taggen und auf diese Weise versteckte funkbasierte Sensoren und Einbruchserkennungstechnik finden und markieren. Anfällig sind hier insbesondere WLAN-Überwachungskameras, deren Standort sich peilen lässt. Mit einem kollaborativen AR-System können die ermittelten Daten für eine Internet-Recherche oder den Rat von Experten irgendwo auf der Welt genutzt werden, um sich Wege zur Umgehung dieser Systeme vorschlagen zu lassen – wenn die Kameras nicht ohnehin offen im Internet zu finden sind[39]. Mit Datenbrillen und solcher Hilfe lassen sich auch untrainierte Einbrecher, aus der Ferne unterstützt, auf sicherheitstechnisch gut geschützte Objekte ansetzen. Ein Experte könnte einer größeren Bande für einen gleichzeitig verübten großen Raubzug zur Verfügung stehen und wäre keinem Verhaftungsrisiko ausgesetzt.

Organisiertes Verbrechen und Terrorismus

Nicht nur in Hollywood-Filmen werden die Abläufe bei Raubüberfällen auf hochwertige Ziele geplant und geübt. Auch terroristische Anschläge werden detailliert und über längere Zeit geplant und vorbereitet.

Unaufdringliche Datenbrillen erleichtern und verbessern die Koordination von Überfällen – insbesondere bei komplexen Abläufen. Mit solchen AR-Werkzeugen lassen sich das Timing perfektionieren und Ablenkungsmanöver effektiver einsetzen. Datenbrillen werden als Werkzeuge explizit dazu entwickelt und genutzt, Handlungen an realen Orten virtuell durchzuspielen oder die Realität in einem Übungsgelände nachzubilden. Mit der Übung an Originalschauplätzen mit unauffälligen Datenbrillen lässt sich ein risikoreicher Raubüberfall besser planen und umsetzen.

Terrorüberfälle größerer Gruppen von Angreifern gab es auf Hotels, Shopping Center, Flughäfen und andere Orte wie in Mumbai, Nairobi[40], Paris, Brüssel und natürlich auf viele Ziele im Irak und Afghanistan. Selbst beim Amoklauf eines Einzeltäters in München 2016 spielte dessen Chat-Kommunikation mit sich selbst eine Rolle bei seiner Selbstdarstellung und der Bewertung durch die Sicherheitsbehörden. Insbesondere die IS-Terrorgruppe experimentiert schon länger mit ferngesteuerten oder durch IT-Einsatz automatisierten Fahrzeugen, Kanonen und anderen Angriffswerkzeugen.[41] Indizien wie diese belegen, dass Gewalttäter und insbesondere Terrorgruppen hinreichende IT-Kenntnisse haben, die auch beim Einsatz von AR-Werkzeugen erforderlich sind.

Wie schon in Militärmanövern der 1990er Jahre demonstriert, könnten koordiniert vorgehende Terrorgruppen mit Datenbrillen eine gemeinsame Lagekenntnis zu Lasten der angegriffenen Zivilbevölkerung ausspielen. Auch bei terroristischen Angriffen ließe sich die Abstimmung von Angriffsabläufen verbessern durch die gemeinsame Kenntnis über Standorte und das Vorgehen der Gruppenmitglieder anhand des visuellen und akustischen Austauschs in Echtzeit.

So könnte eine Terrorgruppe beispielsweise zu Beginn eines Angriffs die Sicherheitskontrollen an verschiedenen Stellen simultan und koordiniert angreifen, bevor Alarm ausgelöst wird. Als zweiten Schritt könnte eine solche Gruppe mehrere Ziele einnehmen und abriegeln, bevor Sicherheitskräfte mobilisiert werden können. Jeder kritische Zugangspunkt ließe sich unter kollaborativer Kontrolle halten – möglicherweise sogar unter Einbeziehung vorhandener Sensoren oder Kameras in das Kommunikationsnetzwerk der Angreifer. Im dritten Schritt könnte eine solche Gruppe Geiseln im Gebäude oder Gelände ohne Kontrollverlust so verteilen, dass eine Geiselbefreiung durch Sicherheitskräfte wesentlich risikoreicher würde. Im Fall einer Befreiungsaktion würde die AR-Vernetzung einer Terrorgruppe den Überraschungseffekt verringern, weil die AR-Systeme selbst von getöteten Terroristen den Mitgliedern ihres Datennetzwerks weiterhin die Videoaufnahmen des ablaufenden Angriffsgeschehens übermitteln können. Zu allem Überfluss ließen sich die Videobilder der Datenbrillen vom Tatort auch noch

als live-stream zu Propagandazwecken verwenden.

Bewertung

Einen solchen Terrorüberfall mit Unterstützung durch Datenbrillen mag man sich nicht ansatzweise vorstellen. Schutz und Sicherheit setzen aber voraus, neue Szenarien durchzuspielen. Die im vorherigen Abschnitt skizzierten Beispiele sind ohne allzu viel Phantasie noch deutlich ausbaufähig. Deswegen ist es durchaus erstaunlich, dass die einfache Übertragung der seit Jahren vorliegenden Erfahrungen aus militärischen Manövern in die Gegenwart von leicht verfügbarer, kollaborativer Datenbrillen-Technologie bisher nicht unter dem Blickwinkel der zivilen Sicherheit gesehen wurde. Mittlerweile ist die Beschaffung und Adaption der nötigen AR-Technik deutlich einfacher zu bewerkstelligen als die Beschaffung von Waffen, Sprengstoff und anderer Militärausrüstung. Es ist daher leider davon auszugehen, dass wir in den nächsten Jahren Szenarien erleben werden, in denen bewaffnete Täter zusätzlich mit Datenbrillen ausgestattet sind, durch die sich eine neue Art von *Datenbrillen-Überfällen* oder gar *Datenbrillen-Terrorismus* entwickeln kann. Wir sollten diese Möglichkeiten nicht ignorieren, sondern heute darüber nachdenken.

Die kollaborativen Einsatzpotenziale von Datenbrillen bergen große Risiken, für illegale Zwecke genutzt zu werden. Die Experimente verschiedener Strafverfolgungsbehörden haben bereits gezeigt, dass diese ihrerseits neue Einsatzszenarien sehen und die Möglichkeiten dieser Technik in der eigenen Praxis erproben wollen. Dabei ist in Erinnerung zu rufen, dass HMDs als nicht-zivile Versionen von Datenbrillen heute schon von militärischen Spezialeinheiten operativ genutzt werden auch in der Bekämpfung ziviler Unruhen. Lediglich der Einsatz marktgängiger, unauffälliger Modelle zu Überwachungszwecken wäre eine wirkliche Neuerung. Einige der möglichen Konsequenzen sind unschwer abzusehen. Andere erfordern grundsätzlichere Überlegungen.

Sollte es dazu kommen, dass Datenbrillen mit ihrer Übermittlung von Videodaten in Echtzeit an zentrale Server zu einer breiteren Nutzung kommen, werden die Sicherheitsbehörden wohl versuchen, auf diese Daten Zugriff zu erlangen mit dem Argument, dass Nutzer der Datenbrillen unwissentlich Aufnahmen eines für die Behörden wichtigen Geschehens machen könnten. Die Durchsuchung des zentral gesammelten Videomaterials von Datenbrillen im Hinblick auf Daten zu einem Tatort oder Tathergang entweder ex post durch Beschlagnahme oder *bei* Verdacht in Echtzeit von allen dort vorhandenen Nutzern dürfte sich zu einer vergleichbar eingesetzten Methode entwickeln wie heute die Auswertung von Überwachungskameras bzw. Handy-Videos.

Verschiedene der zuvor beschriebenen illegalen Nutzungspotenziale dürften mit einer Manipulation insbesondere auch der gemeinsam genutzten Kommunikationsverbindungen einhergehen, um durch eigene Kommunikationskanäle die bei einigen Modellen vorgesehene zentrale Datensammlung zu umgehen. Für die Sicherheitsbehörden wird daraus die Forderung erwachsen, die lokale Kommunikation von Tätergruppen – etwa per WLAN – am Ort eines Geschehens analysieren, überwachen oder stören zu können. Nach IMSI-Catchern und anderem Gerät wird daher der Wunsch nach weiterer Überwachungstechnik laut werden.

Grundsätzlich anders fällt die Betrachtung aus, wenn es um die Frage geht, ob und wie Datenbrillen gegen eine Nutzung für illegale Aktivitäten gesichert werden können, die mit großen Gefahren für die Allgemeinheit, aber auch für die Sicherheitsbehörden verbunden sind. Hier fällt eine Antwort ziemlich ernüchternd aus. Schon heute ist zu viel Software im Umlauf, die für Einzelnutzer und Nutzergruppen die Grundlagen für eine Weiterentwicklung zur Realisierung der vorab beschriebenen kollaborativen AR-Anwendungen schafft. Diese Entwicklung ist nicht mehr einzudämmen.

Was das Verhindern der Anbindung externer Sensorik an Datenbrillen und das AR-typische Taggen von Elementen im Sichtfeld des Nutzers angeht, so ist auch das nur eine Frage der softwareseitigen Datenintegration. Da es regelmäßig um nur wenige Daten geht, ist der Aufwand überschaubar.

Datenbrillen, die mit einem der gängigen Betriebssysteme für den Massenmarkt angeboten werden, sind nicht wirksam gegen Manipulation und Missbrauch zu sichern. Die Hersteller müssten schon an verschiedenen Punkten ihrer Systeme Mechanismen vorsehen, die bei Manipulationen die Datenbrille zur Selbstzerstörung bringen oder eine Deaktivierung von außen erlauben. Wie leicht letzteres umgangen werden kann, hat schon Google Glass gezeigt. Auch hierbei lässt sich daher letztlich nur an der konkreten Implementierung ermessen, ob solche Maßnahmen ausreichen.

Fazit

Gegen die meisten und vor allem die extremsten der beschriebenen illegalen Nutzungsszenarien von Datenbrillen kommen nur sehr wenige technische Mittel infrage. Ideen zur unbegrenzten Datenerhebung wiederum würden massive Grundrechtseingriffe für die Allgemeinheit ohne erkennbaren Nutzen bedeuten.

Zur Prävention von erwartbarem Missbrauch notwendig wäre vielmehr ein *code of conduct* von Selbstbeschränkungsregeln der Anbieter und Software-Entwickler. Hardwareseitig sollte ernsthaft über Manipulationshemmnisse nachgedacht und entsprechende Erschwernisse eingebaut werden. Softwareseitig sollten solche kollaborative Spiele und Anwendungen gar nicht erst auf den Markt gebracht werden, die sich ohne größere Veränderungen für illegale Einsatzszenarien nutzen lassen und so selbst Tätern ohne vorheriges Training die erheblichen Gefährdungsmöglichkeiten einer kollaborativen Datenbrillennutzung eröffnen. Es ist fraglich, ob für eine solche Bewertung die bisherigen Prüfverfahren der Altersfreigabe für Computerspiele ausreichend sind.

Datenbrillen weisen ein erhebliches Potenzial zur Überwachung des Alltags Unbeteiligter auf, das für die Sicherheitsbehörden von großem Interesse ist. Militärische HMDs werden bereits operativ genutzt und dürften zukünftig auch bei Sondereinheiten der Polizei Verwendung finden. Unauffällige zivile Datenbrillen eröffnen den Sicherheitsbehörden erhebliche neue Perspektiven für die Observation und Überwachung. Das sind nur bedingt positive Aussichten, die aber

prinzipiell regelbar und in bestimmten Konstellationen auch nutzbringend sind.

Nicht regelbar ist der Einsatz von Datenbrillen für kriminelle und terroristische Zwecke. Es ist daher umso erstaunlicher, dass diesen Fragen bisher so gut wie nirgendwo nachgegangen wurde und sie für Entwickler und Anbieter keine Rolle zu spielen scheinen.

Bevor wir die ersten *Datenbrillen-Terroristen* erleben müssen, wäre es dringend geboten, daran zu arbeiten, wie diese Technik eingegrenzt werden kann, oder die missbräuchlich nutzbare Arbeit an solchen Geräten aus ethischer Verantwortung heraus einzustellen. Sicherheitsbehörden und Gesetzgeber sind aufgefordert, sich unter operativen und regulatorischen Gesichtspunkten mit den Missbrauchspotenzialen von Datenbrillen auseinanderzusetzen. Die Hersteller schließlich sollten damit konfrontiert werden, dass sie erhebliche Risiken gedankenlos in Kauf nehmen.

Es ist Zeit für eine breite Debatte über die Implikationen eines kollaborativen Einsatzes von Datenbrillen und deren Missbrauch für unsere Gesellschaft, unsere Sicherheit und über mögliche Lösungsansätze – bevor uns die Wirklichkeit äußerst schmerzhafte Lektionen lehrt.

1 Ausgangspunkt dieser Betrachtung ist der Beitrag von Ute Bernhardt: Google Glass: On the implications of an advanced military command and control system for civil society. In: International Review of Information Ethics (IRIE): Cyber warfare, Issue No 19, Vol. 20, December 2013, p. 16-27 http://www.i-r-i-e.net/inhalt/020/IRIE-Bernhardt.pdf

2 Werbung für „Life is Crime" auf: http://www.androidauthority.com/best-ar-apps-and-games-for-android-augmented-reality-584616/; das Spiel ist in Deutschland nicht verfügbar

3 Wilfried Eckl-Dorna: Datenbrille als Logistik-Helfer Neue Chance für Google Glass - in den Lagerhallen von VW, Manager-Magazin, 09.03.2015, http://www.manager-magazin.de/unternehmen/autoindustrie/datenbrille-google-glass-soll-produktivitaet-von-vw-erhoehen-a-1022591.html

4 Mark Hurst: The Google Glass feature no one is talking about; Feb. 28th 2013, http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/

5 "Even share what you see. Live"; http://www.google.com/glass/start/what-it-does/ ; zur Throughglass App: http://glass-apps.org/throughglass-google-glass-app

6 So: Google Glass-Like Products Can Launch For As Low As $400, Forbes, 21.07.2013; http://www.forbes.com/sites/haydnshaughnessy/2013/07/21/google-glass-like-products-can-launch-as-low-as-400/. Zu dieser Zeit wurde bereits über vergleichbare Microsoft-Entwicklungen berichtet: Microsoft Tests Eyewear Similar to Rival Google Glass, Wall Street Journal Online, 22nd Oct. 2013, http://online.wsj.com/news/articles/SB10001424052702304402104579150952302814782. Samsung hatte derweil dazu seinerseits Patente angemeldet: Samsung files patent for Google Glass-like device, San Jose Mercury News, 25.10.2013, http://www.mercurynews.com/business/ci_24386791/samsung-files-patent-google-glass-like-device

7 Beispiele dafür sind Produkte wie die Microsoft Hololens (https://www.microsoft.com/en-us/hololens) und andere in einem Produktvergleich dargestellten: https://www.vrodo.de/augmented-reality-brillen-vergleich/, aber auch ältere Modelle wie die Recon Jet HMD (http://reconinstruments.com/products/jet/), Epiphany Eyewear (https://en.wikipedia.org/wiki/Epiphany_Eyewear), GlassUp aus Italien (http://www.glassup.net/) und das Vuzix Smart Glasses Accessoire für Smartphones (http://www.vuzix.com/consumer/products_m100.html). Sogar Nissan präsentierte ein AR-Gerät auf der Tokyo Motor Show 2013 unter dem Produktname "3E": The 3E View of the Tokyo Motor Show, Nov. 19, 2013, http://blog.nissan-global.com/EN/?p=11271;

8 Doug Bolton: Samsung patents design for ‚smart' augmented reality contact lenses; The Independent, 6.04.2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsung-smart-contact-lenses-patent-a6971766.html unter Bezug auf Samsung is working on smart contact lenses, patent filing reveals, http://www.sammobile.com/2016/04/05/samsung-is-working-on-smart-contact-lenses-patent-filing-reveals/. Die Konzepte dazu sind älter: Babak A. Parviz: Augmented Reality in a Contact Lens. IEEE Spectrum, 1st Sept. 2009, http://spectrum.ieee.org/biomedical/bionics/augmented-reality-in-a-contact-lens

9 MedRec is the first app for Google Glass with face recognition; http://glass-apps.org/medref-google-glass-app. Auf dem CCC-Kongress December 2013 kündigte Lambda Labs eine Gesichtserkennungs-App an, die nicht von Google unterstützt wurde: Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Online, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

10 Siehe Beschreibung und Berichte bei: http://www.google.com/glass/start/

11 Rich Haridy: HoloLens could let flight attendants read your emotions, in: New Altas, 25.05.2017, http://newatlas.com/microsoft-hololens-customer-service-air-new-zealand/49698/

12 Die datenschutzrechtliche Betrachtung kann zurückgreifen auf Überlegungen zu Wearables bei Beschäftigten, siehe dazu auch Thilo Weichert: Wearables – Schnittstelle Mensch und Computer, CuA 10/2016, S. 8 ff.

13 Google Glass Terms of Sale and Use (Dezember 2013); http://www.google.com/glass/terms/

14 ebd.

15 Entwicklerversion der Google Glass per QR-Code gehackt; http://www.heise.de/security/meldung/Entwicklerversion-der-Google-Glass-per-QR-Code-gehackt-1919373.html; based on: Lookout: Sicherheit für die vernetzte Welt: Ein Google Glass-Fallbeispiel; company blog, 17.07.2013, https://blog.lookout.com/de/2013/07/17/sicherheit-fur-die-vernetzte-welt-ein-google-glass-fallbeispiel/

16 Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Online, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

17 Das gilt auch für gleichartige Produkte. Microsoft versuchte, sich eine Datenbrille für Multiplayer-Spiele patentieren zu lassen, so: Microsoft tries to patent AR glasses for multiplayer gaming, engadget, 02.08.2013, http://www.engadget.com/2013/08/02/microsoft-ar-glasses-for-multiplayer-gaming-patent/

18 Simon Parkin: ButtonMasher: First AR games for Google Glass emerge; New Scientist, Nov. 1st, 2013; http://www.newscientist.com/article/dn24505-buttonmasher-first-ar-games-for-google-glass-emerge.html

19 http://www.youtube.com/watch?v=QxG5xNktqw0

20 RoboRaid ist Microsofts Ego-Shooter für die HoloLens, siehe dazu: https://www.microsoft.com/en-us/hololens/apps/roboraid

21 Victor Middleton, Ken Sutton, Bob McIntyre and John O'Keefe IV: Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration

(ATD), Dayton, Oct. 2000, p. 22f. . http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA384680

22 So die Präsentation des britischen Unternehmens Scicon Computer Systems bei der British Army Equipment Exhibition 1984. Diese prototypische Ausrüstung für Soldaten sollte volle AR-Funktionalität mit zusätzlicher Infrarot-Fähigkeit in einem integrierten HMD Display bieten, so: Military Technology, No. 10, 1986, p. 166. Steven M Shaker, Robert Finkelstein: The Bionic Soldier; in: National Defense, April 1987, S. 27 – 32. Head-mounted displays (HMDs) für AR Anwendungen wurden zuerst publiziert als akademisches Paper von Tom Caudell, d.W. Mitzell: Augmented reality: an application of heads-up display technology to manual manufacturing processes; in: Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences, 1992, Vol.2, pp. 659 - 669

23 U.S. Army: TRADOC Pamphlet 525-5: Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, TRADOC Pamphlet 525-5, Fort Monroe, Aug. 1994, S. 2-1ff

24 U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems 2012, S. 108f

25 Im "Warfighter Information Network-Tactical Increment 3" Programm, vgl. U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems Handbook 2013, p. 322f

26 Michael M. Bayer, Clarence E. Rash, James H. Brindle: Introduction to Helmet Mounted Displays, p.47-107; in: Clarence E. Rash, Michael B. Russo, Tomasz R. Letowski, Elmar T. Schmeisser: Helmet-Mounted Displays: Sensation, Perception and Cognition Issues, Fort Rucker, Alabama, 2009; http://www.usaarl.army.mil/publications/HMD_Book09/

27 System „Infanterist der Zukunft – Erweitertes System" (IdZ-ES); http://www.deutschesheer.de/portal/a/heer/start/technik/sonstig/idz/!ut/p/z1/hU5P-C4IwHP0sHbzuNxTTuq0SISQik3SX-mLqmsZzMpX38DE9B0ru9vzygkA-JtWF8LZmrVMDnyjC6vGz86R_bKtn-f4EGCydZNTlIROGNhw-Rego41n-QDDEJYds3PDmNzyIgQK9s569U-Ku0kdwgVnweQlaxppT8qAoyC-XugQqp8uk6a3PEFUM1vXHONnn-qUK2Pabm1hCw_DgIRSQnJUcgv_alS-qM5B-BaF9pAN2XNlHZPEGfAjbLg!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_B8LTL2922D0NE0AC5URLUG3GE7

28 Drittes Auge für Deutsche Soldaten; Spiegel Online, 20.02.2013; http://www.spiegel.de/wissenschaft/technik/militaertechnologie-bundeswehr-will-gladius-system-einfuehren-a-884238.html; sowie auch die Rheinmetall Pressemeldung: https://www.rheinmetall.com/de/media/editor_media/rheinmetallag/press/pressearchiv2012/20120619_beauftragung_gladius_wp_dt.pdf

29 So: Samuel Liles: Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency; Conference on Cyber Conflict, NATO CCD COE Publications, 2010, p. 47-57

30 Mind Commerce: Augmented Reality in the Battlefield 2012 – 2016, July 2012, ADS Report, Amsterdam 2012; https://www.asdreports.com/shopexd.asp?id=32490

31 Matthew Sparks: New York Police Testing Google Glass; The Telegraph, 07.02.2014; http://www.telegraph.co.uk/technology/google/10623753/New-York-police-testing-Google-Glass.html

32 Polizei in Dubai geht mit Google-Datenbrille auf Verbrecherjagd; in: Reuters, 2.10.2014, http://de.reuters.com/article/dubai-google-datenbrille-polizei-idDEKCN0HR19T20141002

33 Peter Welchering: Was die Polizei von morgen über uns weiß, www.heute.de, 15.06.2016, http://www.heute.de/polizeiausruestung-thema-bei-innenministerkonferenz-was-die-polizei-von-morgen-ueber-uns-weiss-43944016.html

34 Terrorismusbekämpfung: Zu wenig Ermittler? ARD Hauptstadtstudio-Blog, 15.10.2016, http://blog.ard-hauptstadtstudio.de/terrorismusbekaempfung-zu-wenig-ermittler/

35 In den ersten sechs Monaten 2016 wurden von den deutschen Sicherheitsbehörden über 210.000 „Stille SMS" zur Ortung von Handys verschickt, vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u.a.: Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2016, vom 09.08.2016, Bt.-Drs. 18/9366, Frage 4

36 Sie gaukeln eine Basisstation vor Ort vor und ermitteln so die Telekommunikationskennungen der Mobilgeräte von unbekannten observierten Personen,

37 Marco Dettweiler; Tillmann Neuscheler: Computersimulierte Menschenströme: Eine Viertelstunde in die Zukunft schauen, in: FAZ, 17.10.2016, http://www.faz.net/aktuell/gesellschaft/ende-der-loveparade/computersimulierte-menschenstroeme-eine-viertelstunde-in-die-zukunft-schauen-11008870.html. Siehe auch: Crowd Management: Smartphone soll Massenpanik verhindern; http://www.golem.de/news/crowd-management-smartphone-soll-massenpanik-verhindern-1209-94331.html

38 So verfügen Landes- und Bundespolizeibehörden neben IMSI-Catchern, die eine Funk-Basisstation vorgaukeln, über Beweissicherungs- und Dokumentationskraftwagen, die Handy-Besitzer metergenau lokalisieren können sollen, siehe Detlef Borchers: Bessere Handy-Ortung für die deutsche Polizei; heise online, 09.08.2014, http://www.heise.de/newsticker/meldung/Bessere-Handy-Ortung-fuer-die-deutsche-Polizei-2289542.html, siehe auch die Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u.a. Neue digitale Überwachungsmethoden, Frage 17 ff

39 Ronald Eikenberg: IP-Kameras von Aldi als Sicherheits-GAU, heise Security, 15.01.2016; https://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html

40 Drama in Einkaufszentrum: Präsident meldet Sieg über Geiselnehmer in Nairobi; http://www.spiegel.de/politik/ausland/praesident-meldet-sieg-ueber-geiselnehmer-in-nairobi-a-924322.html , zu Pakistan und Indien: Hasnain Kazim: Angriff in Lahore: Taliban richten Blutbad in Moscheen an; Spiegel Online, 28.05.2010; http://www.spiegel.de/politik/ausland/angriff-in-lahore-taliban-richten-blutbad-in-moscheen-an-a-697393.html

41 Thomas Gibbons-Neff: Why the Army is worried about insurgents turning to remote-controlled weapons; The Washington Post, 30.08.2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/08/30/insurgent-groups-such-as-isis-are-increasingly-turning-to-remote-controlled-weaponry-army-report-says/; siehe auch: Robert J. Bunker, Alam Keshavarz: Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns; Foreign Military Studies Office, Kansas, August 2016; https://info.publicintelligence.net/USArmy-TeleoperatedSniperRifles.pdf

Heiko Maas

Zusammenleben in der digitalen Gesellschaft

Teilhabe ermöglichen, Sicherheit gewährleisten, Freiheit bewahren

Auszüge aus der Rede des Bundesministers der Justiz und für Verbraucherschutz bei der Konferenz „Digitales Leben –Vernetzt. Vermessen. Verkauft? #Werte #Algorithmen #IoT“ am 3. Juli 2017 in Berlin

Einleitung

Vor fast 150 Jahren wurde hier das „Reichspostministerium“ gegründet. Briefkästen, Telefone und Postkutschen sind die Exponate der Kommunikation in der Vergangenheit. Ich frage mich, wie die Kuratoren es dereinst schaffen werden, dem neugierigen Besucher einen Algorithmus zu präsentieren. Dafür wird man Wege und Möglichkeiten finden.

Im digitalen Zeitalter ist Kommunikation zu einem Phänomen geworden, das kaum noch sichtbar und greifbar ist. Trotzdem bestimmt die digitale Kommunikation immer mehr unseren kompletten Alltag – im Beruf, im Verkehr, im Privatleben und auch in den eigenen vier Wänden. Nicht nur Ausstellungsmacher stehen vor dem Problem, digitale Phänomene sichtbar und greifbar zu machen, sondern wir alle, die wir uns damit befassen. Mangelnde Transparenz ist ein Problem für uns alle. Wir wissen zwar, dass im Internet unzählige persönliche Daten transportiert werden, dass man sie vernetzen und auswerten kann, aber die Einzelheiten bleiben oft völlig unsichtbar.

– Wer weiß schon, welche Daten sein eigenes Smartphone täglich mit wem austauscht?
– Wer rechnet damit, dass selbst der Rhythmus, mit dem wir eine Tastatur bedienen, Auskunft geben kann, in welcher Konsumlaune wir sind?
– Und wer ahnt schon, dass die Fotos, die man auf Instagram veröffentlicht, zur Kalkulation unseres Gemütszustandes ausgewertet werden können?

Wenn Daten, die aus unserem Verhalten gewonnen werden, so weitreichende Schlussfolgerungen erlauben, wäre es sicherlich sinnvoll, Licht in dieses digitale Dunkel bringen. Ich will im Folgenden auf drei Handlungsfelder eingehen, die wir in der Öffentlichkeit und in der Politik beackern müssen, wenn das Zusammenleben in der digitalen Gesellschaft ein gedeihliches sein soll. Es geht darum, die Werte, die unser Zusammenleben in der analogen Welt prägen, auch im digitalen Zeitalter zu wahren. Es geht um nicht mehr, aber auch nicht weniger als Teilhabe, Freiheit und Sicherheit.

– Wir brauchen eine gleichberechtigte Teilhabe am gesellschaftlichen Leben – ohne Diskriminierungen, sondern mit gleichen Chancen für alle.
– Wir müssen die Selbstbestimmung und Handlungsfreiheit des Einzelnen bewahren; Menschen dürfen nicht von Technik beherrscht werden.
– Und wir müssen dafür Sorge tragen, dass die Verantwortlichkeiten für die Sicherheit im Netz klarer werden und die Durchsetzung des Rechts auch im Internet gewährleistet ist.

„On-Life“

Wir alle sind heute vernetzt. Wir alle werden in der digitalen Welt vermessen. Und wir alle müssen aufpassen, dass wir bei allen großartigen Chancen, die das Internet bietet, nicht am Ende genau die Werte verkaufen und opfern, die für eine freiheitliche und demokratische Gesellschaft essenziell sind. Das fundamental Neue an dieser vierten industriellen Revolution ist, dass bisher gültige Grenzen zwischen privat und öffentlich, zwischen „mein“ und „dein“, ja selbst zwischen Mensch und Maschine verschwimmen.

Die immer stärkere digitale Vernetzung führt dazu, dass am Ende alles mit allem kommuniziert und man die Welt nicht mehr in „online“ und „offline“ aufteilen kann. Schon eine Autofahrt mit dem Navigationssystem oder ein Waldspaziergang mit Smartphone am Ohr macht diese Verflechtung deutlich. Der Philosoph Luciano Floridi, der an der Universität Oxford lehrt und arbeitet, nennt diese digitale Lebensform „On-life“. „Onlife“ ist eine Sphäre, in der sowohl Menschen mit Maschinen, Maschinen mit Maschinen und natürlich auch noch Menschen mit Menschen interagieren.

Es geht nicht darum, diese Entwicklung zu beklagen – ganz im Gegenteil. Es geht auch nicht um Kultur-Pessimismus oder Technik-Feindlichkeit. Entscheidend ist vielmehr, dass unsere Gesellschaft diskutiert, wie wir Werte und Regeln, die für unser Zusammenleben wichtig sind, auch in der „Onlife“-Welt erhalten.

Teilhabe

Zunächst zur Frage der gesellschaftlichen Teilhabe: Wie kann auch in der digitalen Welt eine gleichberechtigte Teilhabe am gesellschaftlichen Leben ohne Diskriminierungen, sondern mit gleichen Chancen für alle ermöglicht werden? Wie kann sich der Sozialstaat davor schützen, dass die Schwächeren in unserer Gesellschaft bei der Digitalisierung auf der Strecke bleiben und von gesellschaftlicher Teilhabe ausgeschlossen werden?

Wir produzieren täglich unzählige Daten und rund um die Uhr hinterlassen wir überall Datenspuren. Die Menge der Daten ist so groß wie nie zuvor, es werden in der Zukunft auch noch mehr werden. Wenn diese Big Data digital ausgewertet werden, kann es schnell Gewinner und Verlierer geben. Wenn soziale oder wirtschaftliche Scoring-Verfahren

eingesetzt werden, kann die gefährliche Gleichung lauten: Positive Daten bedeuten Vorteile und Teilhabe – negative Daten Nachteile und Ausgrenzung. Und gar keine Daten können in der digitalen Gesellschaft einer faktischen Nichtexistenz gleichkommen. Wenn zum Beispiel die Bonität von Menschen anhand von Posts bei Facebook und ihrem dortigen „Freundeskreis“ bewertet wird, kann die Abwesenheit von einem Facebook-Profil schnell zu einer ökonomischen Diskriminierung führen. Wenn Daten aus der Vergangenheit über Teilhabe-Chancen in der Zukunft bestimmen, ist das nicht unbedenklich.

Selbstlernende Algorithmen versuchen das Verhalten von Menschen mit immer höherer Genauigkeit vorherzusagen. Schon heute beeinflussen Algorithmen viele Entscheidungen – sowohl im Geschäftsleben als auch politisch und sozial: Der Preis eines Flugtickets, die Kreditwürdigkeit eines Verbrauchers oder der Zugang eines Kunden zu bestimmten Versicherungstarifen werden immer öfter individuell von Algorithmen bestimmt. Und bei bestimmten Kundenhotlines werden angeblich auch nur noch Anrufer durchgestellt, die von einem Algorithmus als wohlhabend eingestuft werden.

Besonders schwierig werden digitale Scoring-Verfahren, wenn sie nicht nur kommerzielle, sondern soziale oder politische Ziele verfolgen: In den USA werden Bewerbungen durch Algorithmen vorsortiert, und die Justiz lässt mancherorts sogar Rückfallwahrscheinlichkeiten von Straftätern von Algorithmen prognostizieren. In China werden in ausgewählten Regionen für jeden Bürger rund 5.000 verschiedene Behördendaten digital zusammengeführt, um seine „soziale Zuverlässigkeit“ zu errechnen. Für die Angepassten gibt es Privilegien, bei abweichendem Verhalten gibt es Sanktionen, vom Ausreiseverbot bis hin zu Bildungsbeschränkungen für die Kinder. Diese Verfahren reduzieren die Menschen auf ihre Vergangenheit und können wichtige Chancen auf einen Neustart in der Zukunft verbauen.

Wir sollten auch mit unserem Glauben an die Objektivität der Technik vorsichtig sein – Algorithmen sind nur so gut wie diejenigen, die sie programmiert haben, und die Datenbasis, mit der sie gelernt haben. Fehler, die dort stattfinden, werden sich in ungeahnter Weise vervielfältigen.

In Australien hat die Regierung vergangenes Jahr ein Experiment mit algorithmischer Entscheidungsfindung gestartet. Die Steuerbehörden haben ihre Bescheide ausschließlich mit Hilfe von Datenabgleichen erstellt: voll automatisiert, ohne Anhörung der Betroffenen, ohne Offenlegung der Entscheidungskriterien. Das Ergebnis war, dass auf Millionen Menschen massive Steuerforderungen zukamen, ohne dass überhaupt klar war, warum. Die australischen Medien nannten diese vom Algorithmus ermittelten angeblichen Schulden denn auch „Robo-Debt“ – „Roboter-Schulden“.

Jenseits des Datenschutzes hat der Einsatz von Algorithmen auch massive gesellschaftliche Effekte. So können soziale Verhältnisse zementiert werden, wenn die Daten, die ein Algorithmus analysiert, bereits selbst Diskriminierungen enthalten. Soziale Ungleichheit kann dann reproduziert und damit im Ergebnis auch verfestigt werden.

In den USA wird zum Beispiel die automatisierte Gesichtserkennung als Beweismittel vor Gericht verwandt. Wissenschaftler haben festgestellt, dass ein Afro-Amerikaner, der vor Gericht steht, bei dieser vermeintlich ganz objektiven Technik einem deutlich höheren Risiko ausgesetzt ist, fälschlicherweise verurteilt zu werden, als ein Nicht-Afro-Amerikaner. Warum? Weil diese Gesichtserkennungsprogramme vor allem mit weißen Testpersonen trainiert werden und deshalb deutlich differenzierendere Ergebnisse bei Weißen liefern, während die Quote falscher Treffer bei Afro-Amerikanern sehr viel höher ist.

Das war ein Beispiel mit besonders drastischen Konsequenzen, aber es gibt auch Diskriminierungen, die weitaus weniger augenscheinlich sind. Wenn heute etwa bestimmte Online-Händler in bestimmte Postleitzahl-Bereiche nicht mehr ausliefern, weil dort die Betrugsfälle besonders hoch sind, dann wird der rechtstreue Besteller in Mitverantwortung genommen und wegen seiner Postleitzahl diskriminiert.

Letztlich sind Algorithmen bloß Werkzeuge. Nicht jedes Werkzeug aber ist für jede Aufgabe geeignet. Je sensibler ein Bereich ist, in dem ein bestimmtes Werkzeug eingesetzt werden soll, desto wichtiger ist es, die Fehleranfälligkeit und Aussagekraft des Algorithmus zu prüfen und zu diskutieren. Im Bereich der Polizeiarbeit oder Strafverfolgung können die Folgen von algorithmischen Fehlern für die Betroffenen verheerend sein. Aber es geht auch um das soziale Zusammenleben.

Seit mehr als zehn Jahren haben wir in Deutschland das AGG – das Antidiskriminierungsgesetz. Wer an der Tür zum Club vom Türsteher wegen seiner Hautfarbe abgewiesen wird, wer wegen einer Behinderung als Hotelgast unerwünscht ist – der kann sich mit diesem Gesetz gegen diese Diskriminierungen wehren. Ein digitales AGG, ein digitales Antidiskriminierungsgesetz könnte hilfreich sein – gegen digitale Diskriminierung und für vorurteilsfreies Programmieren. Technischer Fortschritt darf eben nicht zu gesellschaftlichem Rückschritt führen, und deshalb wäre ein Ordnungsrahmen nötig, der viel Raum für Innovationen bietet, der aber genauso den Einsatz von diskriminierenden Algorithmen verhindert.

Selbstbestimmung

In der schönen neuen Welt der Algorithmen müssen wir auch die Selbstbestimmung bewahren. Die Grundfrage lautet hier: Wie schützen wir in Zeiten der Digitalisierung die Selbstbestimmung und die Handlungsfreiheit des Einzelnen? Wie verhindern wir, dass Menschen nicht allein der Technik unterworfen werden?

Vielleicht kennen Sie die englische Comedy-Serie „Little Britain“. Da gibt es einen Sketch mit dem Titel „Computer says No“. Verschiedene Bürger besuchen ein Reisebüro, sind bei der Bank oder bei der Anmeldung im Krankenhaus. Ihre Anliegen werden überall von Mitarbeitern aufgenommen und in den Computer eingegeben. Aber was immer sie wollen, sie bekommen überall die gleiche Auskunft: „Computer says No“. Warum und wieso entschieden wurde, bleibt das Geheimnis des Algorithmus. Eine Begründung gibt es nichts. Lediglich Mitarbeiter, die nur wiederholen können: „Computer says No“

Was als Comedy lustig daherkommt, verweist auf ein ernstes Problem der digi-

talen Welt: Bis zu welchem Grad sind wir bereit, unsere Handlungsfreiheit durch Algorithmen beschneiden zu lassen? Und wie schaffen wir die Transparenz, die Voraussetzung für jede Selbstbestimmung ist? Wie weit ist es mit diesen Maximen eigentlich noch her, wenn etwa unser Such- und Leseverhalten im Netz so ausgewertet wird, das uns ständig Vorschläge gemacht werden, die auf unser bisheriges Verhalten abgestimmt sind?

Diesen gleichen Effekt der permanenten Selbstbestätigung fördern soziale Netzwerke, wenn einzelne Botschaften durch Algorithmen sortiert, personalisiert oder gefiltert werden. Indem Algorithmen menschliches Verhalten auf vorbestimmte Bahnen lenken, können sie die Selbstbestimmung und Handlungsfreiheit des Einzelnen durchaus auch einschränken. Früher hieß das Tunnelblick. Heute sind es die „Echokammer" und die „Filter-Blase", die dafür sorgen, dass wir oftmals nur noch auf Positionen treffen, die uns in der eigenen Meinung bestärken – egal wie absurd die im Einzelfall auch sein mag. Selbst die Anhänger der „Flat Earth"-Theorie bekommen permanent neue Belege aus dem Netz, die ihre Theorie bestätigen, dass die Erde tatsächlich eine Scheibe ist.

Wenn Sie eine Zeitung oder Zeitschrift von vorne bis hinten durchblättern, stoßen Sie immer wieder auf Themen und Thesen, die Sie bislang nicht kannten und nun für sich entdecken können, ohne nach ihnen gesucht zu haben. Solche Neuentdeckungen verhindern die Echokammern und Filter-Blasen im Netz: Überraschungen, Irritationen, abweichende Meinungen werden ausgeblendet, damit sich der Nutzer in seiner eitlen Selbstbespiegelung und Selbstbejahung sogar noch sonnen kann. Diese Form der Weltflucht und des Verzichts auf Selbstbestimmung ist für das Zusammenleben und den Zusammenhalt in einer Gesellschaft durchaus kontraproduktiv. Es ist ja nicht so, dass in der analogen Welt die Menschen immer parallel die FAZ und das „Neue Deutschland" lesen, um ihren Horizont zu weiten. Aber der Unterschied ist, dass in der analogen Welt die Ausrichtungen dieser Blätter transparent sind und die Entscheidungen für das eine oder andere Medium bewusst und selbstbestimmt getroffen werden.

Wenn aber unter dem Mantel der technischen Neutralität und Objektivität Trefferlisten und die Anzeige von Nachrichten und Postings politisch manipuliert werden, dann bleibt die demokratische Selbstbestimmung auf der Strecke.

Ein Transparenzgebot für Algorithmen wäre hilfreich, damit Nutzerinnen und Nutzer verlässlich einschätzen können, ob das Netz versucht, sie zu beeinflussen, und damit sie selbstbestimmt entscheiden können, welche Filter und Personalisierungen sie in der digitalen Welt akzeptieren wollen und welche nicht.

„Computer says No" – das passt nicht zu einem freiheitlichen Rechtsstaat. Im Rechtsstaat sind alle Entscheidungen begründungspflichtig. Denn nur so kann überprüft werden, ob die Grundlagen, auf denen sie getroffen wurden, richtig, rechtmäßig und auch verhältnismäßig sind. Eine solche Überprüfbarkeit brauchen wir auch, wenn Algorithmen Entscheidungen vorbereiten.

Auch im digitalen Raum muss sich der freie gesellschaftliche Diskurs vollziehen können. Und gerade die politische Willensbildung muss frei bleiben von digitaler Manipulation aus dem Verborgenen heraus.

Sicherheit

Es bleibt der letzte Aspekt der Sicherheit. Wie können wir gewährleisten, dass die digitalen Prozesse und Produkte sicher sind, und dafür sorgen, dass geltendes Recht im Netz eingehalten wird? Es geht um digitale Produktsicherheit, aber auch um Rechtssicherheit.

Wenn digitale Produkte und Prozesse Sicherheitslücken aufweisen, dann müssen die Verantwortlichkeiten zwischen Herstellern, Dienstleistern und Verbrauchern klarer sein, als es bisher der Fall ist. Denn die Risiken müssen fair verteilt sein. Erst vor wenigen Tagen mussten Unternehmen und Behörden auf der ganzen Welt einen massiven Cyberangriff mit Schadprogrammen auf ihre Netzwerke abwehren. Und je mehr alltägliche Geräte im sogenannten „Internet der Dinge" digital miteinander kommunizieren, desto höher sind die Sicherheitsrisiken, derer sich viele Nutzerinnen und Nutzer noch gar nicht bewusst sind. Um europaweit geltende Vorschriften zur IT-Sicherheit, die verpflichtende Mindestanforderungen definieren, werden wir nicht herumkommen. Außerdem könnte durch die Einführung eines freiwilligen Gütesiegels für internetfähige Produkte mehr Transparenz über die jeweiligen Sicherheitseigenschaften hergestellt werden.

Risikoverteilung ist immer eine Frage der Verteilung von Verantwortung. Aber Verantwortung kann man nur für Risiken tragen, die man kennen und beherrschen kann. Sicherheitslücken bei der Programmierung sind dem Zugriff des Durchschnittsverbrauchers völlig entzogen, und deshalb ist es nicht fair, wenn die Folgen solcher Sicherheitslücken einseitig auf den Verbraucher abgewälzt werden.

Neben der Produktsicherheit muss es auch die Sicherheit geben, dass das geltende Recht auch im Internet eingehalten wird. Schnelle Überprüfungs- und Abhilfemöglichkeiten, eine effektive Rechtsdurchsetzung sind zwingende Voraussetzung, damit die Menschen Vertrauen in die digitale Welt fassen und ein Leben „onlife" tatsächlich auch Zukunft hat.

Das Internet darf kein rechtsfreier Raum sein. Und es darf auch keinen rechtsschutzfreien Raum geben. Unsere Gesellschaft darf ihren Anspruch, die Digitalisierung zu gestalten, nicht aufgeben und vor den kommerziellen Interessen der globalen Internet-Riesen nicht die Segel streichen. Die Digitalisierung ist eine großartige und faszinierende Entwicklung. Ich wollte in keiner anderen Epoche leben als im digitalen Zeitalter. Aber wir müssen gemeinsam dafür Sorge tragen, dass Werte, die schon unsere Vorfahren erstritten und erkämpft haben, nicht leichtfertig untergraben werden.

Schluss

Gleichheit und Freiheit – das sind die Werte, um die es im Wesentlichen geht. Und Transparenz ist der Garant dafür, um Diskriminierungen zu verhindern und Selbstbestimmung zu sichern. Deshalb brauchen wir mehr Transparenz von Algorithmen. Wir brauchen auch eine Rechtsdurchsetzung, Aufsicht und die Kontrolle von Transparenz. Wir brauchen auch mehr wissenschaftliche Expertise, denn wie soll die Gesellschaft der Technik Regeln setzen, wenn der Sachverstand dafür nur in betroffe-

nen Unternehmen vorhanden ist? Deshalb sollte die nächste Bundesregierung eine „Digital-Agentur“ gründen, um im Austausch mit Wissenschaft, Wirtschaft und Verbrauchern mehr Expertise zu erlangen – über Algorithmen, über das Internet der Dinge und das Leben in der digitalen Welt.

Die oberste Maxime unseres Zusammenlebens ist und bleibt die Würde eines jeden Menschen. „Computer says No“ – das ist mit dieser Maxime nicht vereinbar. Denn zur Menschenwürde im digitalen Zeitalter gehört vor allem, dass niemals ein Mensch zum bloßen Objekt von Technik oder auch Algorithmen werden darf.

Quelle:

https://www.bmjv.de/SharedDocs/Reden/DE/2017/07032017_digitales_Leben.html

Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 13. September 2017

Bündnis für mehr Videoaufklärung – 10 Gründe, warum Sie nicht unterschreiben sollten



Webseite des Bürgerbündnisses für mehr Videoaufklärung und mehr Datenschutz

Das Bürgerbündnis für mehr Videoaufklärung und mehr Datenschutz hat einen Gesetzesentwurf für ein „Artikel-Gesetz für mehr Sicherheit und mehr Datenschutz in Berlin“ vorgestellt, über den in einem Volksbegehren entschieden werden soll. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, rät Berliner Bürgerinnen und Bürgern aus folgenden Gründen davon ab, die Initiative zu unterstützen:

1. Mit Datenschutz hat das nichts zu tun!

Das Bündnis gibt als eines seiner Hauptanliegen vor, den Datenschutz beim Einsatz von Videoüberwachungstechnik verbessern zu wollen. Ein Blick in den Gesetzesentwurf zeigt jedoch, dass das Gegenteil der Fall ist. Überwachungsmaterial soll zunächst in verfassungsrechtlich anfechtbarer Weise anlasslos auf Vorrat gespeichert werden. Durch sog. intelligente Techniken soll tiefer als bisher in das Persönlichkeitsrecht der Bürgerinnen und Bürger eingegriffen werden. Darüber hinaus sollen Hinweise auf Überwachungsmaßnahmen unter bestimmten Voraussetzungen entfallen können. Diese Vorschläge lassen sämtliche datenschutzrechtliche Grundprinzipien völlig außer Acht.

2. Niemand soll anlasslos verdächtigt werden!

Die Initiatoren möchten es der Polizei mit dem Gesetzesentwurf ermöglichen, für einen pauschalen Zeitraum von mindestens einem Monat anlasslos umfassendes Bild- und Tonmaterial zu speichern. Solche Maßnahmen stellen alle Berliner Bürgerinnen und Bürger in Generalverdacht. Verfassungsrechtlich ist eine solche Speicherung von Daten auf Vorrat höchst bedenklich.

3. Videoüberwachung macht die Stadt nicht sicherer!

Die Initiative hat zum Ziel, Berlin sicherer zu machen. Mehr Kameras tragen dazu nicht bei. Gewalttäter, die im Affekt handeln, lassen sich von einer Kamera nicht abhalten. Terroristen

könnten sich durch sie gar angespornt fühlen. Aber auch Kriminelle, die ihre Taten vorab planen, werden durch den Einsatz von Überwachungskameras nicht von ihrem Ansinnen absehen, sondern Mittel und Wege finden, der Überwachung zu entgehen (z. B. durch einfaches Verhüllen des Gesichts durch Kapuzen oder Ähnliches).

4. Auch wer nichts zu verbergen hat, ist betroffen!

Gerne wird argumentiert, wer nichts zu verbergen hat, habe auch nichts zu befürchten. Das ist falsch. Insbesondere der Einsatz von sog. intelligenter Überwachungstechnik könnte künftig auch unbescholtene Bürgerinnen und Bürger in die Gefahr bringen, sich verdächtig zu machen, indem sie sich scheinbar ungewöhnlich verhalten oder sich zufällig in der Nähe von Straftätern aufhalten. So kann z. B. häufiges Rolltreppenfahren an Bahnhöfen als auffällig eingestuft werden, da sich auch Taschendiebe entsprechend verhalten; auch ein längeres Warten auf eine Verabredung könnte problematisch werden. In Kombination mit der Abspeicherung biometrischer oder in sonstiger Weise personenbeziehbarer Daten können Menschen so unvermittelt als verdächtige Person gelten und ins Fadenkreuz von Ermittlungen geraten.

5. Lauschangriff auf Berlin!

Das Bündnis sieht nicht nur den vermehrten Einsatz von Videoaufnahmen vor. Öffentliche Orte, wie Verkehrsmittel, Gerichte, Religionsstätten und Friedhöfe sollen künftig auch akustisch überwacht werden dürfen. Der Gesetzeswortlaut lässt theoretisch auch eine Überwachung von Einkaufszentren, Kaufhäusern, Restaurants, Schwimmbädern, Museen und sogar Privatgebäuden und -geländen von öffentlichem Interesse zu. In weiten Bereichen der Berliner Innenstadt könnten Bürgerinnen und Bürger sich dann nicht mehr sicher sein, wer ihnen wann zuhört.

6. Identitätsdiebstahl kann lebenslange Folgen haben!

Das Bündnis will die Entwicklung sog. intelligenter Videotechnik fördern. Darunter fallen auch Verfahren, die mit biometrischen Daten arbeiten, wie die automatische Gesichtserkennung. Die Risiken dieser Technik sind gravierend. Anders als z. B. Passwörter sind biometrische Daten nicht veränderbar. Geraten sie einmal in die falschen Hände, kann das für die Betroffenen lebenslange Folgen haben. Im Besitz biometrischer Daten könnten Kriminelle auch noch nach Jahren Online-Einkäufe auf Kosten der Opfer tätigen oder sich Zugang zu fremden Systemen verschaffen.

7. Die Missbrauchsgefahr ist real!

Je mehr Daten erhoben und je länger sie gespeichert werden, desto mehr steigt auch die Gefahr des Missbrauchs. Große Datenhacks in der Vergangenheit, z. B. im Telekommunikationsbereich, haben gezeigt, wie anfällig technische Systeme für unerlaubte Zugriffe sind. Insbesondere biometrische Daten sind aufgrund der mit ihnen verbundenen eindeutigen und regelmäßig unabänderlichen Zuordnungsmöglichkeit zu den Betroffenen als äußerst sensibel einzustufen. Ihre Erhebung und Speicherung ist daher nur innerhalb enger verfassungsrechtlicher Grenzen zulässig.

8. Die Datenschutzaufsicht ist und bleibt unabhängig!

Mit dem vorgeschlagen Gesetz soll ferner ein öffentliches Institut für Kriminalprävention gegründet werden. Unter der Aufsicht der für Forschung zuständigen Senatsverwaltung soll dieses Institut unter anderem Bürgerinnen und Bürger in Sachen Datenschutz beim Einsatz von Videotechnik beraten und Auskunft über die Anwendbarkeit der datenschutzrechtlichen Normen erteilen. – Eine systematische, wissenschaftlich fundierte Überprüfung des bisherigen Einsatzes von Videoüberwachungsmaßnahmen in Berlin ist zwar durchaus wünschenswert, sie muss aber ergebnisoffen und durch unabhängige Einrichtungen erfolgen. In der vorgeschlagenen Form unterliegt die Errichtung des vorgeschlagenen Instituts nachhaltigen verfassungsrechtlichen Bedenken. Die Datenschutzberatung ist nach höherrangigem Recht eine Kernaufgabe der Datenschutzaufsichtsbehörden. Deren Unabhängigkeit ist verfassungsrechtlich und europarechtlich geschützt.

9. Es fehlt schon an der Gesetzeskompetenz!

Durch die Ausweitung der Videoüberwachung soll insbesondere die Verfolgung von Straftaten verbessert werden. Dieses Anliegen kann jedoch nicht mit einem Berliner Volksbegehren durchgesetzt werden. Die Aufgabe der Strafverfolgung ist der Berliner Polizei durch die Strafprozessordnung, also ein Bundesgesetz, zugewiesen. Auf Grundlage des Berliner Allgemeinen Sicherheits- und Ordnungsgesetzes kann die Polizei ausschließlich im Rahmen der Gefahrenabwehr Maßnahmen treffen, die für die Verfolgung von Straftaten vorsorgen. Eine Regelung zur anlasslosen Überwachung zum Zweck der Strafverfolgung ist im Polizeirecht ausgeschlossen.

10. Es geht um viel mehr…

Bei der Frage, ob die Initiative unterstützt werden sollte, geht es nicht bloß um die Entscheidung über ein paar Kameras mehr oder weniger. Die Debatte wirft vielmehr die Frage auf, wie wir künftig leben wollen. Der politische Trend, als Reaktion auf die Probleme in unserer Gesellschaft die Überwachungsinfrastruktur immer weiter auszubauen, ist ein zweifelhafter Ansatz. Anstelle Probleme von der Wurzel her anzugehen und Fragen nach den Ursachen zu stellen, werden elementare Grundfreiheiten unserer demokratischen Gesellschaft zur Disposition gestellt.

Maja Smoltczyk:

„Ob und inwieweit Freiheitsrechte eingeschränkt werden dürfen, um Straftaten vorzubeugen oder aufzuklären, bedarf einer sachlichen, öffentlichen Diskussion und einer sorgfältigen Abwägung aller betroffenen Aspekte. Wer solche Maßnahmen jedoch in einem Gesetzesentwurf mit dem Titel „mehr Sicherheit und mehr Datenschutz“ verpackt, verkauft dem Bürger eine Mogelpackung. Dass das vorgeschlagene Gesetz zu mehr Sicherheit führt, ist mehr als zweifelhaft. Dass es mit dem Datenschutz nicht vereinbar ist, steht fest.“

Quelle:
https://www.datenschutz.de/buendnis-fuer-mehr-videoaufklaerung-10-gruende-warum-sie-nicht-unterschreiben-sollten/

Leserbrief von Patrick Breyer und eine Replik von Thilo Weichert

Patrick Breyer schreibt: „Im Teil „Rechtsprechung“ habt ihr auf S. 110 der DANA 2/2017 dankenswerterweis über das BGH-Urteil zu IP-Adressen berichtet. Leider kann die Überschrift (´IP-Adressenspeicherung für Sicherheitszwecke zulässig`) und der erste Satz den Eindruck erwecken, der BGH habe die Speicherung von Surfprotokollen zur Abwehr von Sicherheitsrisiken für zulässig erklärt.

Aus dem inzwischen vollständig vorliegenden Urteil ergibt sich, dass die Internetnutzung mitsamt der IP-Adresse nur protokolliert werden darf, ´soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf`. Um diese Abwägung vorzunehmen, muss das Landgericht Berlin nun zunächst prüfen, ´ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist`, insbesondere welches ´Gefahrenpotenzial` die Internetportale des Bundes aufweisen. Wenn der BGH die Erforderlichkeit und das Ergebnis der Abwägung als offen ansieht, kann man dem Urteil eine Entscheidung über die Zulässigkeit noch nicht entnehmen.

Pressemitteilung von Patrick Breyer:

In meinem Grundsatz-Rechtsstreit gegen die Vorratsspeicherung der Internetnutzung (auch Surfprotokollierung oder Internet-Tracking genannt) hat der Bundesgerichtshof nun die Begründung zu seinem viel beachteten Urteil vom 16. Mai vorgelegt (Az. VI ZR 135/13).

Danach unterliegt die IP-Adresse als Identifikationsmerkmal beim Surfen im Netz dem Datenschutz. Anbieter von Internetportalen dürfen die Internetnutzung mitsamt der IP-Adresse nur protokollieren, ´soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf`. Um diese Abwägung vorzunehmen, müsse das Landgericht Berlin zunächst prüfen, ´ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist`, insbesondere welches ´Gefahrenpotenzial` die Internetportale des Bundes aufweisen. Der Bund verzichte nach eigenen Angaben bei einer Vielzahl von Portalen mangels ´Angriffsdrucks` auf eine Speicherung. Das Interesse an einer protokollierungsfreien Internetnutzung sei allerdings im Fall dynamischer IP-Adressen ´nach den bisherigen Feststellungen eher gering` zu veranschlagen, weil deren Identifizierung ´an enge Voraussetzungen gebunden` sei. Anders liege es bei statischen IP-Adressen, deren Zuordnung zu bestimmten Anschlüssen einer allgemein zugänglichen Datei zu entnehmen sei.

Mein Kommentar als Kläger: Ob eine massenhafte Aufzeichnung unseres Internet-Nutzungsverhaltens gestattet ist und, wenn ja, wie lange, lässt der Bundesgerichtshof offen. Doch eins wird deutlich: Offenbar konnte ich den Richtern noch nicht ausreichend vermitteln, dass uns eine Aufzeichnung unserer Internetnutzung nackt im Netz macht.

Was ich lese, schreibe und wonach ich suche, spiegelt meine privatesten und intimsten Interessen, Überzeugungen, Vorlieben und Schwächen wieder – doch davon findet sich kein Wort im Urteil. Der ständige Eindruck von Überwachung und die permanente Sorge vor möglichen Konsequenzen – egal, ob sie tatsächlich eintreten oder nicht – macht eine unbefangene Information und Diskussion über das Netz unmöglich. Eine Vorratsspeicherung unserer Internetnutzung setzt intimste Informationen über unsere Persönlichkeit inakzeptablen Risiken von Datenverlust, Datenmissbrauch oder falschem Verdacht aus. Nur nicht gespeicherte Daten sind sichere Daten. Das Bundesverfassungsgericht hat schon in seinem Urteil zur Vorratsdatenspeicherung betont, dass die Internetnutzung nicht inhaltlich festgehalten und damit rekonstruierbar bleiben darf. Unser Leben wird immer digitaler, aber es darf damit nicht immer gläserner werden!

Ein gerichtliches Sachverständigengutachten für das Landgericht Berlin hat schon vor Jahren ergeben, dass – unabhängig vom ‚Angriffsdruck‘ – ‚für die Absicherung von IT-Systemen eine Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden’ als eine massenhafte Surfprotokollierung existieren.[1] Im Zeitalter internationaler Netzwerke auf IT-Sicherheit durch Abschreckung (‚Generalprävention‘) zu setzen, ist illusorisch und entbehrt jeder gesetzlichen Grundlage. Ein effektiver Schutz vor Angriffen ist alleine durch technische Absicherung der Systeme möglich.“

[1] Sachverständigengutachten (Seite 10), http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf

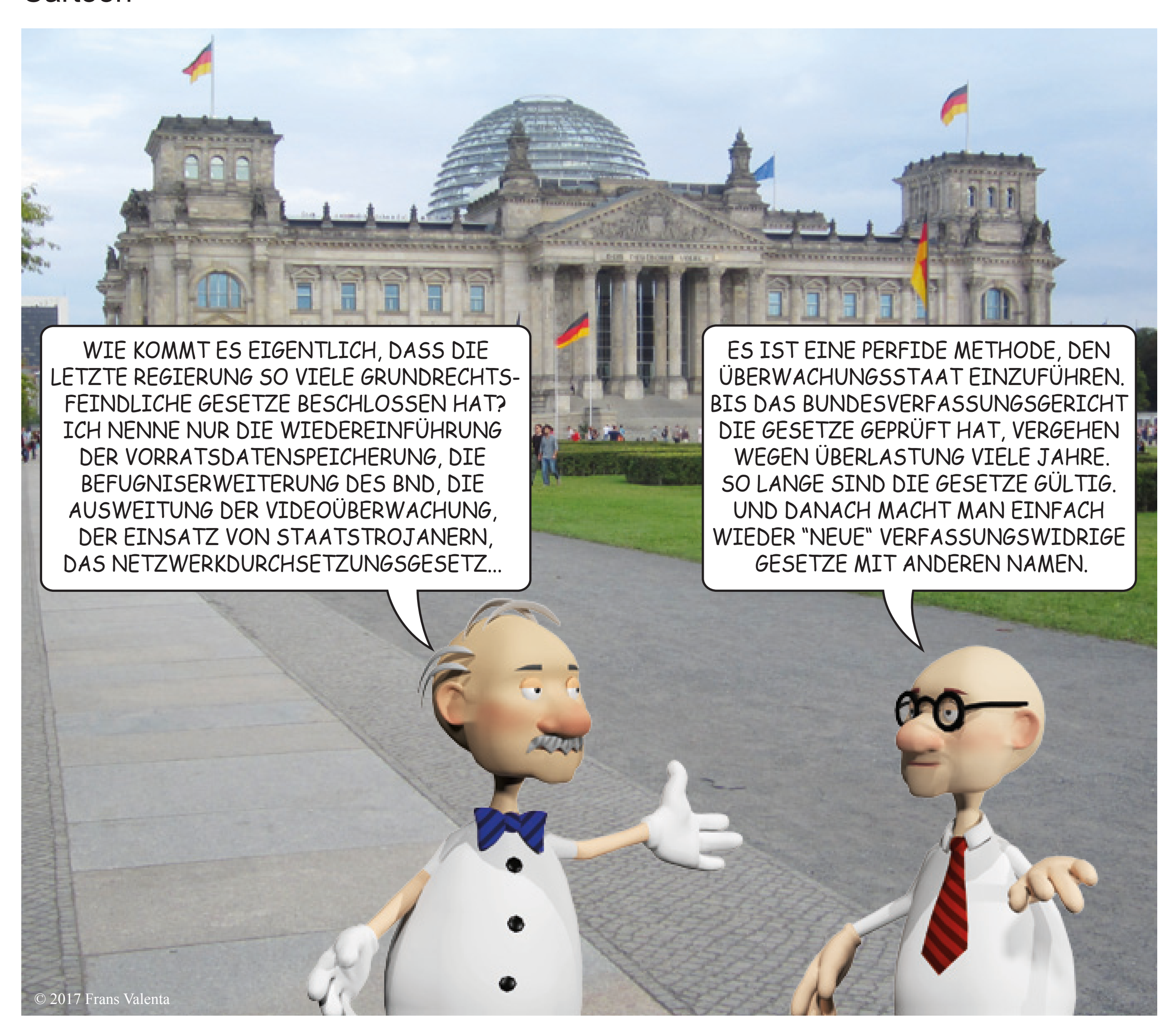
Antwort von Thilo Weichert auf diesen Leserbrief:

„Patrick Breyers Position ist von Vorgestern. Sie ist von einem schwarz-weißen Weltbild geprägt, das leider über zwei Jahrzehnte die Diskussion um die Vorratsspeicherung von Telekommunikations- (TK-) Metadaten prägte. Es geht schon lange nicht mehr um `nackt´ vs. `anonym´, es ging noch nie um `Generalprävention´, heute sollte es um konkrete Angriffsabwehr gehen. Diese Diskussion wurde glücklicherweise vom Bundesverfassungsgericht, vom Europäischen Gerichtshof (EuGH) und nun in Reaktion auf den EuGH vom

Bundesgerichtshof (BGH) auf eine rationalere Ebene gebracht. Es geht also nicht um `Vorratsdatenspeicherung – ja oder nein´. Datenspeicherungen sind weder Teufelszeug noch Allheilsmittel. Es geht vielmehr um Datenminimierung sowie darum, Grundrechte miteinander abzuwägen, Verhältnismäßigkeitsfeststellungen vorzunehmen und informationelle Eingriffe durch technisch-organisatorische oder auch durch materiellrechtliche Vorkehrungen erträglich zu machen, wenn sie für wichtige Zwecke erforderlich sind. Dass eine kurzfristige Speicherung von IP-Adressen aus Gründen der IT-Sicherheit erforderlich und auch verhältnismäßig sein können, wird von vernünftigen Datenschützern nicht mehr bestritten. So wurde über Jahre die einwöchige Speicherung von Metadaten durch die Telekom toleriert. Richtig ist es, über die Dauer, die Modalitäten und die Zwecke der Speicherung von TK-Metadaten zu diskutieren. Dabei ist es auch relevant, dass IP-Adressenspeicherungen zur Aufdeckung und zur Verhinderung von Datenschutzverstößen notwendig sein können. Dass insofern das aktuelle deutsche Gesetz zur Vorratsspeicherung von TK-Daten über das verhältnismäßige Maß hinausgeht, ist inzwischen nicht nur von der Rechtsprechung, sondern auch von der Verwaltungspraxis, leider nicht von der Regierungspolitik, erkannt worden.

Die Haltung von Breyer ist problematisch, wenn sie von ihm zur Spaltung der Datenschutzbewegung genutzt wird und wenn er diskursive Positionen als Verrat auszugrenzen versucht. Sie hat zur Folge, dass er sich selbst aus dem Dialog ausgrenzt. Es kommt nicht von ungefähr, dass Breyer seit über zwei Jahren die öffentliche Diskussion über einen rationalen Umgang mit TK-Metadaten in Kiel verweigert. Man könnte den Eindruck haben, dass ihm Effekthascherei wichtiger ist als adäquate Lösungen.“

Cartoon



Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Spracherkennungsprogramme im BAMF geplant

Das Bundesamt für Migration und Flüchtlinge (BAMF) hat Spracherkennungsprogramme zur Identifizierung von Asylsuchenden abgelehnt, die es im Frühjahr 2016 angeboten bekam. Eine Erprobung sei unter anderem wegen Vorbehalten beim Datenschutz unterblieben. Mit den Programmen hätten, so Pressemeldungen unter Berufung auf eine interne Quelle aus dem BAMF, die 14 falschen Identitäten des späteren Attentäters Anis Amri enttarnt werden können. Den Berichten zufolge hatten mehrere IT-Unternehmen aus Deutschland und Israel der Behörde entsprechende Angebote unterbreitet, wovon mindestens eines der Unternehmen aus Israel Kontakte zum israelischen Geheimdienst besitze. Viele Geheimdienste setzen Spracherkennungsprogramme ein. Moderne Programme versuchen anhand von Gesprächsanalysen die Herkunft eines Sprechers mit hoher Wahrscheinlichkeit zu identifizieren. Es könne nicht nur festgestellt werden, ob jemand in seiner Muttersprache spricht. Sogar die Zuordnung des Dialektes zu einzelnen Regionen sei möglich. Das Bundesinnenministerium bestätigte, dass die Behörde mittlerweile den Markt für „Systeme der Sprach- und Gesichtserkennung“ eruiert. Ob und wann eine Testreihe geplant sei, wurde jedoch nicht bekanntgegeben.

Rund 60% der Asylantragstellenden erscheinen beim Bundesamt oder den Ausländerbehörden ohne Papiere. Laut einer McKinsey-Studie sind die Abschiebungshindernisse oft „vorgetäuscht oder selbstverschuldet herbeigeführt“. Die bisherige Methode, Gutachter zu bestellen, ist ausgesprochen umständlich und kostspielig. Zudem hätten Dolmetscher häufig falsche Loyalitäten. Das BAMF formulierte in einer Stellenausschreibung: „Wir erwarten von Ihnen eine genaue und neutrale mündliche Übersetzung der Gesprächsinhalte“ (Daniel Karmann, Datenschutz: Bamf lehnte Spracherkennungsprogramme ab, jungefreiheit.de 26.05.2017).

Bund

Städte- und Gemeindebund gegen „Datenkapitalismus“

Der deutsche Städte- und Gemeindebund fordert ein Regelwerk zur Nutzung von Daten, so Hauptgeschäftsführer Gerd Landsberg: „Wir brauchen ein Digitalgesetzbuch, am besten ein europäisches. Darin muss geordnet sein, wem welche Daten gehören, wer daran welche Rechte hat und wie der Datenschutz gesichert ist.“ Google und Apple verschafften sich bereits Zugriffe auf lukrative Daten. „Das kann zu einem Digitalkapitalismus führen. Den müssen wir verhindern.“ Die Digitalisierung sei eine Riesenchance für die Kommunen. „Nur sie haben so viele Daten von den Bürgern. Wir wissen, wie viel Wasser sie verbrauchen, wie groß die Wohnung ist, welches Auto sie fahren. Das muss man im Sinne der Bürger nutzen.“ Für Parkhausbetreiber könnten zum Beispiel Verkehrsdaten sehr interessant sein. Der baden-württembergische Gemeindetagspräsident Roger Kehle verglich die Digitalisierung mit der industriellen Revolution: „Wir müssen uns auf den Weg machen, diese Dinge zu gestalten“ (Gemeindebund warnt vor „Digitalkapitalismus“, www.stimme.de 10.08.2017).

Bundesweit

Amazon-Apotheken wegen Schweigepflichtverletzung abgemahnt

Mitte Juni 2017 flatterten in die Büros von 41 Versandapotheken, die ihre Produkte über Amazon anbieten, Abmahnungen wegen Verstoßes gegen den Datenschutz mit Fristsetzung 23.06.2017 12 Uhr mittags. Amazon reagierte auf die Abmahnungen mit einer kurzfristig einberufenen Telefonkonferenz. Viele der abgemahnten Versandapotheken hatten sich zuvor hilfesuchend an die Amazon-Zentrale in München gewendet. Auf der einen Seite der Leitung saßen die Amazon-Anwälte, am anderen Ende die Rechtsanwälte der Versandapotheken. Doch statt einer klaren Antwort habe es nur so etwas wie ein „Brainstorming“ gegeben, berichtete ein enttäuschter Teilnehmer. Die Situation sei „unbefriedigend unklar“ geblieben. Irgendwie sei man sich dann doch einig geworden, dass kein Verstoß gegen den Datenschutz vorliege. Eine Musterantwort hatten die Amazon-Anwälte nicht parat, so dass jede abgemahnte Apotheke selbst entscheiden musste. Eine Apotheke hatte zunächst einmal ihren Webshop vom Netz genommen: „Unsere Internetseite wird aktuell neu gestaltet. Für aktuelle Informationen, mehr Kundenservice und attraktive Angebote. Wir bitten um Ihr Verständnis und etwas Geduld. Besuchen Sie uns bald wieder.“ Andere Versandapotheken wiesen dagegen den Vorwurf des Verstoßes gegen den Datenschutz zurück.

Ins Rollen gebracht hat die Aktion Hermann Vogel jr., Inhaber der Winthir-Apotheke in der Nymphenburger Straße in München. Dass seit Mai KundInnen in München den Expressdienst „Prime Now“ auch für Apothekenpro-

dukte nutzen können, brachte für ihn das Fass zum Überlaufen. Vogel und seine Anwälte sind der Ansicht, dass der Vertrieb über Amazon gegen den Datenschutz verstößt. Die Kanzlei fordert von den abgemahnten Apotheken, alle apothekenpflichtigen Produkte vom Amazon-Portal zu entfernen. Branchenkenner schätzen, dass inzwischen 40% des OTC-Geschäfts der Versandapotheken über Amazon läuft. Dies wird von einem Versandhändler bestätigt: „Von dort kommt jede zweite Bestellung." Mit der Unterlassungserklärung wäre dieser Kanal verstopft.

Die Abmahnung wird damit begründet, dass es verboten ist, Apotheken von Nicht-Apothekern zu betreiben. Insbesondere Gesundheitsdaten gehörten zu den besonders schützenswerten Informationen, deren Erhebung deshalb besonders strengen Vorschriften unterliege. Die abgemahnten Versandapotheken seien bei Amazon registriert und böten dort Medikamente an. Darunter befänden sich auch apothekenpflichtige Arzneimittel wie Aspirin, Grippostad und Canesten. Amazon sei bekanntlich in Luxemburg ansässig. In der eigenen Datenschutzerklärung führe Amazon aus, „dass und welche Daten erhoben werden" und dass Amazon Daten auch weitergebe. Beim Kauf von Arzneimitteln gehörten dazu auch Namen und Adresse des Bestellers und der Name des Medikaments: „Aus dem Namen des Medikaments lassen sich ganz unschwer Rückschlüsse auf die Beschwerden des Bestellers ziehen."

Es komme zu einer Datenerfassung durch ein Unternehmen, das keinen beruflichen Geheimhaltungspflichten unterliegt. Es fehle an der notwendigen vorherigen Zustimmung der Patienten zur Datenweitergabe: „Damit handeln Sie als Apotheker, der sich dieses besonderen Vertriebskanals ‚Amazon' bedient, rechtswidrig." Es liege ein klarer Rechtsverstoß vor. „Informationen über Arzneimittelkäufe und damit über Krankheiten von Patienten sind wohl völlig unstrittig besonders geschützte personenbezogene Daten." Die abgemahnten Amazon-Apotheken handelten vorsätzlich. In der eigenen Datenschutzerklärung weise die Versandapotheke darauf hin, dass sie verpflichtet sei, vor einer Datenverarbeitung eine Einverständniserklärung einzuholen. Dies „zeigt deutlich, dass hier durch Sie sogar vorsätzlich gehandelt wird." Daher stehe Vogel jr. ein Unterlassungsanspruch zu (Klein, Abmahnungen: High-Noon bei Amazon, www.apotheke-adhoc.de, 23.06.2017).

Baden-Württemberg

Dashcam-Aufnahmen führen zu Schadenersatzanspruch

Erstmals ist es in einem obergerichtlichen Verfahren zur einer Verwertung von Aufnahmen einer sog. Dashcam in einem Kfz-Schadenersatzprozess gekommen, nachdem das Oberlandesgericht (OLG) Stuttgart die Bilder einer solchen im Auto angebrachten Kamera, die laufend das Verkehrsgeschehen aufzeichnet, als Beweismittel zuließ.

Es ging dabei um den Zusammenstoß zweier Autos an einer Engstelle: Der Kläger fuhr an ein paar rechts parkenden Autos vorbei, die Fahrerin eines entgegenkommenden Fahrzeugs sah ihn zu spät, so dass es zu einer Kollision mit einem mehrere tausend Euro teuren Blechschaden kam. Auf den Bildern, die im Gerichtssaal vorgeführt wurden, konnte man genau erkennen, wie die Frau in letzter Sekunde das Steuer nach rechts riss. Zudem ließ sich die Geschwindigkeit des Autos aus den Aufzeichnungen ablesen. Ohne Kamera, so hatte ein Sachverständiger im Verlaufe des Verfahrens festgestellt, wären die Details des Unfalls nicht aufklärbar gewesen.

Die Verwertung solcher Dashcam-Bilder ist bisher stark umstritten. Mehrere unterinstanzliche Gerichte lehnten deren Verwertung aus Gründen des Datenschutzes ab, die Mehrzahl hat sich indes dafür ausgesprochen. Das OLG Stuttgart hatte zuvor die Nutzung der Bilder im Rahmen eines Bußgeldverfahrens mit Beschluss vom 4.5.2016 erlaubt (4 Ss 543/15). Offen war bisher, ob eine Verwertung auch für eine Schadensersatzklage zulässig ist. Der Deutsche Verkehrsgerichtstag hatte sich im vergangenen Jahr für einen zurückhaltenden Umgang mit Dashcam-Bildern eingesetzt. Er plädierte für Kameras, deren Aufnahmen nach kurzer Zeit automatisch überschrieben werden.

Die Position des OLG Stuttgart könnte zu gravierenden Änderungen in der Praxis führen: Bisher leiden Prozesse um Verkehrsunfälle oft an ungenauen Zeugenaussagen und sich widersprechenden Behauptungen. Das wurde auch in der OLG-Verhandlung deutlich. Ausschlaggebend für das OLG Stuttgart war nach den Worten des Senatsvorsitzenden Hans-Joachim Rast, dass die Dashcam lediglich die Straße filmt, nicht aber in die Privat- oder gar Intimsphäre eindringt; der Eingriff in das Persönlichkeitsrecht sei relativ gering. „Im öffentlichen Raum muss jeder damit rechnen, fotografiert oder gefilmt zu werden." Deshalb seien die Interessen desjenigen, der seine Ansprüche aus einem Autounfall durchsetzen möchte, deutlich gewichtiger.

Ein letztinstanzliches Urteil des Bundesgerichtshofs wird es im konkreten Verfahren nicht geben, da die Stuttgarter Verhandlung ohne Urteil endete: Unter dem Eindruck der Aufnahmen einigten sich die beiden Beteiligten auf einen Vergleich. Das Ergebnis zeigte übrigens, dass die Dashcam nicht immer nur dem nützt, der sie an seiner Windschutzscheibe angebracht hat. Der Fahrer musste im konkreten Fall ein Drittel des Schadens selbst übernehmen, weil er nach Auffassung des Gerichts vorsichtiger an den parkenden Autos hätte vorbeifahren müssen (Janisch, Richter lassen Auto-Kamera als Beweismittel zu, SZ 18.07.2017, 1).

Bayern

Verfassungsbeschwerde gegen Überwachungsbefugnisse

Die Gesellschaft für Freiheitsrechte (GFF) hat Anfang August 2017 beim Bundesverfassungsgericht (BVerfG) in Karlsruhe gegen „uferlose Befugnisse" des bayerischen Staatsschutzes Verfassungsbeschwerde eingelegt. Es geht vor allem um Online-Durchsuchungen, Messenger-Überwachung und den Zugriff auf Telekommunikations- (TK-)Daten. Gut ein Jahr zuvor

ist die Reform des bayerischen Verfassungsschutzgesetzes in Kraft getreten. Die Beschwerde richtet sich gegen einige der darin enthaltenen umstrittenen Regeln, u. a. gegen das Zugriffsrecht des Landesamts für Verfassungsschutz (LfV) auf die von TK-Anbietern aufbewahrten Verbindungs- und Standortdaten. Innenminister Joachim Herrmann (CSU) hatte bei dem Gesetzesbeschluss eingeräumt, mit diesem bundesweiten Novum bei der derzeit ausgesetzten Vorratsdatenspeicherung an rechtsstaatliche Grenzen zu gehen.

Das LfV soll, so die GFF, auf die sensiblen Informationen „unkontrollierten Zugriff bekommen", was vom Bundesgesetzgeber keinesfalls vorgesehen gewesen sei. Auch weitere mit der Novelle verknüpfte und nun angegriffene Kompetenzen beachteten vom Bundesverfassungsgericht aufgestellte Vorgaben nicht. So könnten heimliche Online-Durchsuchungen oder eine Quellen-TK-Überwachung von WhatsApp und Co. teils schon „gegen bloße Kontakt- und Begleitpersonen angeordnet werden". Damit drohe eine weitgehende Ausforschung durch Staatstrojaner, der Kernbereich privater Lebensgestaltung und berufliche Vertrauensverhältnisse würden nicht hinreichend geschützt.

Die vom Mainzer Staatsrechtler Matthias Bäcker verfasste Klage wendet sich auch gegen die enthaltene Lizenz zum großen Lauschangriff per akustischer Wohnraumüberwachung sowie für den Einsatz verdeckter Ermittler. Unzulässig weit gehen demnach ferner die Befugnisse des Bayerischen Staatsschutzes, erhobene Daten an inländische und ausländische öffentliche Stellen, aber auch an Private und an Unternehmen zu transferieren. Das Verfahren hat laut der GFF Signalwirkung: Es gelte, die anderen Länder davon abzuhalten, vergleichbare Bestimmungen einzuführen und damit verbundene tiefe Grundrechtseingriffe zu erlauben. Beschwerdeführer sind mehrere Personen, die Organisationen angehören, die in Bayern bereits geheimdienstlich überwacht wurden (Krempl, Verfassungsbeschwerde gegen Bayerntrojaner und ausgeweitete Vorratsdatenspeicherung, www.heise.de 08.08.2017).

Bremen, Brandenburg u. a.

Sommer und Hartge wiedergewählt

Die brandenburgische Landesdatenschutzbeauftragte Dagmar Hartge trat am 29.06.2017 ihre dritte Amtszeit an, nachdem sie an diesem Tag für weitere sechs Jahre mit großer Mehrheit ohne vorherige Debatte und Anhörung vom brandenburgischen Landtag im Amt bestätigt wurde. Sie wird 2018 über 32 Personalstellen verfügen, vor zehn Jahren waren es 18. Hartges Behörde war am Zertifizierungsprojekt „Trusted Cloud" des Bundeswirtschaftsministeriums beteiligt und setzt auf das Standard-Datenschutz-Modell (SDM), um „Privacy by Design" künftig besser umsetzen zu können. Nach Ansicht von Hartge muss das SDM nach der Erprobungsphase auch rasch auf europäischer Ebene etabliert werden.

Die Bremer Datenschutzbeauftragte Imke Sommer wurde zwei Wochen zuvor von der Bremer Bürgerschaft für weitere acht Jahre im Amt bestätigt. Auch hier gab es vor der Wahl keine öffentliche Anhörung der Kandidaten. Bisher sehen die gesetzlichen Regelungen in Deutschland kein transparentes Bestellungsverfahren vor. Die Verwaltungsjuristin Sommer will sich für eine stärkere Transparenz von Algorithmen in Big-Data-Anwendungen einsetzen: „Um entscheiden zu können, welche Nutzung unserer Daten in Ordnung ist und welche nicht, müssen wir die wesentlichen Eigenschaften der vermeintlich smarten Scorings kennen, die die überall über uns zusammengesammelten Daten interpretieren." Nur „wenn wir unzulässige Verknüpfungen kennen, können wir sie zurückweisen."

Ein Gutachten des „Netzwerks Datenschutzexpertise" stellt fest, dass die Neigung, eine AmtsinhaberIn wiederzuwählen, stark ausgeprägt ist. Die 2016 verabschiedete europäische Datenschutzgrundverordnung, die ab Mai 2018 umgesetzt werden muss, verlangt ein fair gestaltetes, „transparentes Verfahren". Möglich wäre dies durch eine öffentliche Ausschreibung, eine öffentliche Anhörung der Bewerber sowie eine öffentliche parlamentarische Aussprache vor der Wahl. Auch gab es sowohl in Brandenburg wie auch in Bremen mehrere Kandidaten. Doch eine öffentliche Anhörung sowie Aussprache gab es jeweils nicht.

In Sachsen-Anhalt darf der derzeitige Amtsinhaber Harald von Bose nicht zum dritten Mal gewählt werden. Seine Amtszeit ist bereits seit März 2017 abgelaufen, doch hat sich der Landtag noch nicht um eine Neubesetzung gekümmert. Von Boses Amtsvorgänger Klaus-Rainer Kalk musste noch über ein Jahr nach Ablauf seiner zweiten Amtszeit die Behörde führen. In Baden-Württemberg war der Posten des Amtsleiters 2016 fast acht Monate lang vakant, bevor Stefan Brink zum Leiter gewählt wurde. Aus anderen Bundesländern sind noch längere Übergangszeiträume bekannt (Schulzki-Haddouti, Brandenburger Landesdatenschutzbeauftragte wiedergewählt, www.heise.de 29.06.2017; siehe auch das Portrait von Schulzki-Haddouti auf https://www.datenschutzbeauftragter-online.de/datenschutzbeauftragte-brandenburg-zaeh-kompromissbereit/10853/).

Nordrhein-Westfalen

Fitnesscenter McFit lässt mit Daten zahlen

McFit plant in Oberhausen auf 55.000 Quadratmetern in den ehemaligen Thyssenhallen den weltweit größten Fitness-Park mit dem Projekttitel „The Mirai", was unter Rückgriff auf das Japanische „Die Zukunft" bedeutet. Gemäß einer Pressemitteilung beschwört McFit die „Vision" eines Ortes der „Inspiration, Kreativität und Motivation". Fitness soll für jeden Menschen zugänglich gemacht werden - unabhängig von Herkunft, Alter oder Einkommen. Deshalb soll es auch keine monatlichen Mitgliedsbeiträge geben. McFit-Gründer Rainer Schaller erklärte: „Durch das direkte Zusammenbringen von Industrie und Menschen wird jedem die Möglichkeit geboten, Fitness ohne Mitgliedsbeiträge zu betreiben."

Verdienen möchte McFit bei dem mehrere Millionen Euro kostenden Projekt dadurch, dass die bei den Nutzenden anfallenden Daten ausgewertet werden. Die Antwort auf die Frage, ob die Daten

verkauft werden: „Das ist so nicht korrekt. Wir werden keine Daten verkaufen. Wir wollen bei The Mirai fundierte Grundlagenforschung betreiben und eine einzigartige Bestandsaufnahme der Trainierenden einholen, die bisher - wenn überhaupt - nur sehr lückenhaft existiert.“ Bislang gebe es „kaum Daten, die für die Gesundheits-, Fitness- und viele artverwandten Branchen sehr nützlich sind“. Man plane eine umfassende Studie in Zusammenarbeit mit Datenschutzbeauftragten, „um alle Bestimmungen einzuhalten und für alle Beteiligten ein bestmögliches Ergebnis zu erzielen“.

Auf die Frage, was mit den Daten der Trainierenden passiert, erklärte Mirai-Geschäftsführer Ralph Scholz lediglich: „Wir werden die Datenschutzbestimmungen selbstverständlich einhalten und uns auch gegen Hackerangriffe schützen. Bitte haben Sie Verständnis, dass wir zum jetzigen Zeitpunkt noch keine weiteren Details veröffentlichen können“ (Sieben, Mega-Sportzentrum „The Mirai“ in Oberhausen: Will McFit mit deinen Fitnessdaten Geschäfte machen? www.derwesten.de 31.08.2017).

Datenschutznachrichten aus dem Ausland

Weltweit

Banken nutzen Problem-Datenbank „World-Check“

Der weltweit agierende Informations- und Medienkonzerns Thomson-Reuters, zu dem auch die Nachrichtenagentur Reuters sowie verschiedene Fachinformationsdienste gehören, betreibt die Datenbank World-Check. World-Check ist einer von wenigen großen Anbietern für Informationen über potenziell problematische Kunden für Banken und Finanzdienstleister, sogenannte politisch exponierte Personen, kurz PEPs, Schwerkriminelle, Geldwäscher und Terrorverdächtige. Die Datenbank enthält mehr als zwei Millionen Profile zu Einzelpersonen und Organisationen. Vor allem Banken haben ein großes Interesse daran, zu erfahren, mit wem sie Geschäfte machen, um nicht in Geldwäsche oder Terrorfinanzierung verwickelt zu werden. Besteht der Verdacht, dürfen sie sogar ein Basiskonto verweigern.

Zugriff auf World-Check haben nur Unternehmen die zuvor zahlreiche Checks durchlaufen haben und Verschwiegenheitserklärungen abgeben. Thomson-Reuters behauptet, 49 der 50 größten Banken nutzten den Dienst. Das Abo hierfür soll bis zu eine Million Euro jährlich kosten. 2016 stieß der amerikanische Sicherheitsexperte Chris Vickery auf mehr als zwei Millionen Profile aus dieser Datei mit Stand aus dem Jahr 2014, die durch ein Sicherheitsleck auf einen Internet-Server gelangt waren. World-Check wirbt mit: „Finden Sie versteckte Risiken“.

Ein gewaltiges Risiko ist die Datei für diejenigen, die in ihr gespeichert sind. Dabei handelt es sich offensichtlich oft um Unschuldige, also um Menschen und Organisationen, gegen die einmal ergebnislos ermittelt wurde, oder die umstritten und unbequem sind, aber nicht kriminell, etwa die Menschenrechtsorganisation Human Rights Watch oder die Tierschützer von Peta. Lokalpolitiker, Dissidenten sowie Kinder und Verwandte von politischen Persönlichkeiten tauchen auf sowie Verstorbene. Der Eindruck, dass Profile auf teils zweifelhaften Quellen beruhen und mangelhaft gepflegt sind, entstand für einen journalistischen Rechercheverbund, der Einblick in die Datenbank erlangte. Wer bei Dienstleistern wie World-Check einen Eintrag hat, womöglich noch mit einem so schweren Vorwurf wie Terror-Verbindungen, kann schon bei einfachen Bankgeschäften große Schwierigkeiten bekommen.

Ein Beispiel hierfür ist Andrej Holm, der bis Sommeranfang 2017 von seiner Speicherung keine Ahnung hatte. Er wollte ein zusätzliches Girokonto eröffnen, um die Buchhaltung zu vereinfachen und seine freiberufliche Tätigkeiten gesondert abzurechnen. Holm ist ein renommierter Soziologe und war kurzzeitig Baustaatssekretär in der Berliner Landesregierung. Weil Holm keine Kontogebühren zahlen wollte, wandte er sich an die Norisbank. Er bekam eine Kontonummer und eine EC-Karte, kurz darauf aber einen Brief: Die Norisbank wolle ihn nun doch nicht als Kunden, es werde keine Geschäftsbeziehung geben. Als Holm nachfragte warum, erhielt er keine Antwort. Jahrelang blieb unklar, warum die Norisbank Holm nicht als Kunden haben wollte. Eigentlich hatte er die Sache auch fast schon vergessen. Nun aber gibt es offenbar eine Erklärung dafür: Der linke Wissenschaftler und Politiker bekam sein Konto wohl deshalb nicht, weil er wegen „mutmaßlicher Terror-Verbindungen“ auf einer internationalen schwarzen Liste steht.

2006 hatte die Bundesanwaltschaft Holm im Verdacht, mitverantwortlich für linke Brandanschläge zu sein. Ende August 2007 waren sich die Ermittler so sicher, dass sie Holm nach ausgiebiger Überwachung wegen des Verdachts auf Mitgliedschaft in einer terroristischen Vereinigung verhafteten. Drei Wochen saß er in Haft, dann kam er wieder frei. Im Sommer 2010 wurden die Ermittlungen schließlich komplett ohne Verurteilung oder Strafe eingestellt. Holm wurde für seine Haft entschädigt, auf seinen Arbeitsplatz an der Uni hatte die Sache keinen Einfluss.

Für Staat und Justiz war er unschuldig, nicht aber für World-Check. Die gesichtete Version der Datenbank stammt aus dem Jahr 2014, also vier Jahre, nachdem alle Vorwürfe gegen Holm fallen gelassen wurden. In der Kartei findet sich davon aber kein Wort, das letzte Update zu seinem Profil stammt vom 29.07.2008. Thomson-Reuters wirbt für seinen Dienst damit, dass neben Algorithmen auch 250 Analysten monatlich 25.000 neue Profile anlegen und 40.000 Profile auf den neuesten Stand bringen. Holms Profil enthält Fehler: So heißt es dort, er sei auf Kaution auf freiem Fuß, tatsächlich aber hatte er Haftverschonung erhalten, was juristisch ein bedeutender Unterschied ist. Auf Anfrage gab die Norisbank an, Namenslisten zu

prüfen, beantwortete aber konkrete Fragen nicht und berief sich hierzu auf den Datenschutz.

Konfrontiert mit den Recherche-Ergebnissen, äußert sich auch Thomson-Reuters – ebenfalls mit Verweis auf den Datenschutz – nur sehr zurückhaltend. Die Informationen für World-Check stammten vor allem aus Hunderten Regierungs- und Justizdatenbanken, von Aufsichts- und Strafverfolgungsbehörden, der EU und den Vereinten Nationen. Weitere Informationen, etwa aus Weblogs, flössen nur zur Bestätigung anderer Erkenntnisse ein und seien klar gekennzeichnet. Die Erkenntnisse würden dann von Teams spezialisierter Mitarbeiter zusammengeführt und abgeglichen. Zudem bedeute ein Eintrag bei World-Check nicht, dass jemand tatsächlich schuldig sei.

Hamburgs Datenschutzbeauftragter Johannes Caspar erklärte, dass derartige Datenbanken nach deutschem Recht „hierzulande so nicht zulässig“ sind. Es handle sich um eine Auskunftei, in der nur bestimmte überprüfte Daten gesammelt werden dürfen. Daher sei auch der Abruf von Daten durch deutsche Unternehmen bei World-Check rechtlich problematisch. Dies hindert aber viele Institute in Deutschland, beispielsweise die meisten großen Privatbanken sowie fast alle Genossenschaftsbanken, nicht, den Dienst zu nutzen. Gerechtfertigt wird dies damit, dass die Institute gesetzlich verpflichtet sind, besonders sorgsam bei Geschäften mit politisch exponierten Personen zu sein. Wer in diese Kategorie fällt, ist offen. Die Deutsche Kreditwirtschaft als Dachverband der Branche forderte deshalb auf Anfrage die „Schaffung verbindlicher und abschließender Listen“ durch die EU. Auch in der Branche ist World-Check wegen der ungenügenden Datenqualität umstritten.

Andrej Holm kommentierte seinen Fall: „Ich weiß, was es heißt als Terrorverdächtiger zu gelten. Das zieht schnell weite Kreise, das sieht man ja an diesem Fall.“ Das sei viel beunruhigender als der Schaden, den er hatte. Es bleibe ein „Gefühl des Ausgeliefertseins“. Er verstehe den Wunsch, Schwerkriminelle zu überwachen. „Aber ein unbewiesener oder sogar widerlegter Verdacht darf niemals ausreichen, um auf solch einer Liste zu landen.“ Holm bekam damals übrigens noch ein zweites Konto bei seiner alten Hausbank, der Berliner Sparkasse (Radomsky/Klofta, Auf der schwarzen Liste der Banken, www.sueddeutsche.de 24.06.2017 = Gefangen auf der schwarzen Liste, SZ 24./25.06.2017, 25).

Weltweit

Google will auf Mail-Inhaltskontrolle für Werbezwecke verzichten

1,2 Milliarden Menschen haben einen E-Mail-Account bei Google. Dieses Gmail-Angebot ist nicht nur erfolgreich, sondern wird aus Verbraucherschutz- und Datenschutzgründen heftig kritisiert, u. a. weil alle eingehenden E-Mails automatisch gescannt wurden, um personalisierte Werbung anzuzeigen. Damit soll jetzt Schluss sein. Im Firmenblog kündigte die Google-Managerin Diane Greene an, dass Privatnutzende keine Werbung mehr angezeigt bekommen sollen, die auf den Inhalten der E-Mails ihres Gmail-Kontos basiert. Wer bislang etwa Suchaufträge bei Immobilienportalen erstellt hatte und sich passende Mietwohnungen per E-Mail schicken ließ, dem blendete Google möglicherweise Werbeanzeigen von Immoscout, Immowelt oder WG-Gesucht ein.

Die Ankündigung enthält keine Angaben über den Zeitpunkt der geplanten Änderung. Gemäß Greene soll die Umstellung „im Laufe des Jahres“ erfolgen. Dann soll sich die Werbung, die innerhalb von Gmail eingeblendet wird, nach den allgemeinen Anzeigeneinstellungen des jeweiligen Google-Nutzers richten. Hierfür bietet Google seit 2 Jahren die Seite „Mein Konto“ an, wo alle Einstellungen für Privatsphäre und Sicherheit gebündelt sind. Nutzende können z. B. den Such- und Wiedergabeverlauf von Youtube-Videos löschen, die Weitergabe von persönlichen Daten an das Analyse-Werkzeug Google Analytics untersagen oder eben interessenbezogene Werbung deaktivieren. Auf der Unterseite „Einstellungen für Werbung“ können Nutzende den Schieberegler auf „Aus“ stellen.

Unabhängig von Googles Ankündigung werden also alle Gmail-Nutzenden weiterhin Werbung geschaltet bekommen. In der Standardeinstellung richten sich die Anzeigen nach früheren Google-Suchen, vermuteten soziodemographischen Merkmalen, dem Standortverlauf des Smartphones und anderen Faktoren. Künftig soll der E-Mail-Inhalt insofern keine Rolle mehr spielen. Wer überhaupt keine personalisierten Anzeigen ausgeliefert bekommen möchte, muss das unter „Mein Konto“ angeben.

Der Verbraucherzentrale Bundesverband (vzbv) hatte Anfang 2016 Google wegen der Scan-Praxis, ohne dass die Nutzenden ausreichend darüber aufgeklärt werden, abgemahnt. Bereits 2011 hatte der damalige Berliner Datenschutzbeauftragte Alexander Dix festgestellt, dass die Praxis von Google das Fernmeldegeheimnis verletzt. Offiziell begründet das Unternehmen den Kurswechsel mit dem Erfolg von G Suite, einem kostenpflichtigen Angebot für Geschäftskunden. Dort verzichtet Google darauf, E-Mails zu Werbezwecken zu scannen. Angeblich führten die unterschiedlichen Vorgehensweisen zu Verwirrung bei Unternehmen, die sich für G Suite interessierten, weshalb Google die Praxis vereinheitlichen wolle, um Missverständnisse zu verhindern und potenzielle Geschäftskunden nicht abzuschrecken.

Auch in Zukunft werden Algorithmen E-Mails bei Gmail analysieren, um Spam und Malware auszufiltern, Informationen für Googles persönlichen Assistenten zu gewinnen oder E-Mails automatisch in bestimmte Kategorien einzusortieren. Alternativen mit besserem Datenschutz sind etwa die deutschen Anbieter Posteo und Mailbox.org oder Protonmail aus der Schweiz. Diese kosten zwischen einem und vier Euro pro Monat und finanzieren sich nicht durch Werbung (Google will E-Mails nicht mehr zu Werbezwecken scannen, www.sueddeutsche.de 25.06.2017; Hurtz, Schluss mit Scannen, SZ 26.06.2017, 21).

Frankreich

CNIL verhängt erstmals Bußgeld wegen Datenpanne

Der Autovermieter Hertz muss 40.000 € an die französische Staatskas-

se zahlen, weil Daten von über 35.000 KundInnen offen über seine Webseite zugänglich waren. Die Datenschutzaufsichtsbehörde, die Commission Nationale de l'Informatique et des Libertés (CNIL), nutzte damit erstmals eine neue Sanktionsmöglichkeiten bei Datenschutzpannen. Seit November 2016 kann die CNIL gemäß dem „Gesetz für eine digitale Republik" Datenschutzverstöße mit Geldbußen ahnden. Zuvor durfte sie nur Warnungen aussprechen. Beim erstmaligen Gebrauch dieser neuen Option traf es den Autovermieter Hertz mit der 40.000 €-Strafe.

Oktober 2016 waren persönliche Daten wie Name, Kontaktdetails und Führerscheinnummern von 35.357 Website-Nutzenden bei www.cartereduction-hertz.com frei zugänglich. InhaberInnen einer Rabattkarte der Firma können über das Portal Vergünstigungen in Anspruch nehmen. Mitarbeiter der CNIL hatten durch einen Hinweis von dem Leck erfahren. Sie setzten Hertz umgehend von dem Fund in Kenntnis. Die Zuständigen dort alarmierten die Vertragsfirma, die für die Entwicklung der Seite zuständig war. Diese habe umgehend die nötigen Schritte eingeleitet, um das Datenleck zu stopfen.

Bei genaueren Untersuchungen fanden die Prüfer nach eigenen Angaben heraus, dass die Panne die Folge eines Fehlers während eines Serverwechsels war. Dabei sei eine Codezeile gelöscht worden, sodass die ausgefüllten Formulare der Teilnehmer an dem Rabattprogramm wieder angezeigt werden konnten. Bei dem eingeleiteten Sanktionsverfahren und der nun gegen die französische Tochterfirma des US-Konzerns verhängten Strafe hat die CNIL nach ihrer Lesart berücksichtigt, dass der Autoverleiher rasch reagiert, gut mit dem Amt zusammengearbeitet sowie ein umfassendes Datenschutzaudit eingeleitet habe. Von Mai 2018 an können Aufsichtsbehörden aller EU-Mitgliedsstaaten gemäß der Datenschutz-Grundverordnung Bußgelder bis zu 20 Millionen Euro beziehungsweise bei Konzernen bis zu vier Prozent des weltweiten Umsatzes des Vorjahres verhängen (Krempl, Frankreich: Datenschutzbehörde verhängt erstmals Geldstrafe für Datenpanne, www.heise.de 28.07.2017).

Schweden

Regierungskrise nach „Datenskandal"

In Schweden hat die Auslagerung sensibler Daten eine Krise der rot-grünen Minderheitsregierung und eine Kabinettsumbildung ausgelöst. Unter dem Druck der Opposition traten am 27.07.2017 zwei Minister zurück, verbunden mit der Ankündigung des sozialdemokratischen Regierungschefs Stefan Löfven, er werde das Land nicht in eine politische Krise stürzen. Er werde nicht zurücktreten und auch keine Neuwahl ausrufen. Ministerpräsident Löfven nahm die Rücktrittsgesuche von Innenminister Anders Ygeman und Infrastrukturministerin Anna Johansson an. Verteidigungsminister Peter Hultqvist hingegen bleibe trotz der Rücktrittsforderung der Opposition im Amt, denn er trage keine Verantwortung für den Skandal.

Den Oppositionspolitikern zufolge soll auch Hultqvist es versäumt haben, Lövfen über das Datenleck informiert zu haben, obwohl er selbst davon bereits Anfang 2016 gewusst habe. Auslöser für die Empörung der Opposition war die Entscheidung der staatlichen Verkehrsbehörde, ihre IT-Verwaltung 2015 an den Computerkonzern IBM auszulagern, um Geld zu sparen. IBM wiederum beauftragte Subunternehmen unter anderem in Tschechien und Rumänien. Deren IT-Spezialisten hatten damit trotz fehlender Sicherheitsüberprüfung Zugang zu sensiblen Daten des schwedischen Militärs und der Führerscheinbehörde, u. a. das Register mit den Daten aller Fahrzeuge und FührerscheinbesitzerInnen im Land inclusive Foto. Laut Schwedens Nachrichtendienst Säpo gehörten zu den Daten auch Angaben über das Straßennetz, Brücken, das U-Bahnsystem sowie über militärische Fahrzeuge. Gemäß Medienberichten könnten auch Daten über vorbestrafte oder verdächtige Personen betroffen sein, die Wege von gepanzerten Fahrzeugen für Personen, die unter besonderem Schutz stehen, über verdeckte Ermittler und über die Routen von Geldtransportern.

Welches Ausmaß das Leck tatsächlich hatte, ist noch ungewiss. Jonas Bjelfvenstam, der neue Chef der Verkehrsbehörde, nannte die Medienberichte übertrieben und ungenau. Die Server hätten stets in Schweden gestanden und die Behörde habe die meisten geheimen Register militärischer Fahrzeuge selbst betreut. Die Verkehrsbehörde beteuerte zudem, dass bisher nichts auf einen Missbrauch der Daten hindeute. Es solle darauf hingewirkt werden, dass nur noch autorisierte Personen Zugang zu ihnen haben.

Der Vorgang war öffentlich geworden, weil die frühere Chefin der Verkehrsbehörde Maria Ågren im Januar 2017 wegen der Auslagerung gekündigt und zu einer Geldstrafe verurteilt worden war. Sie hatte die Datenauslagerung unter Zeitdruck vorangetrieben und Warnungen des Nachrichtendienstes ignoriert. Premierminister Löfven gab an, erst im Januar von der Sache erfahren zu haben. Säpo untersuchte den Fall, erste Ergebnisse wurden Ende Juli 2017 veröffentlicht. Löfven bezeichnete die Vorgänge als „Desaster": „Das ist unglaublich ernst. Es ist eine Verletzung des Gesetzes und bringt schwedische Bürger in Gefahr."

Verteidigungsminister Hultqvist erklärte, er habe „alle nötigen Maßnahmen" ergriffen, um die Folgen für das Militär zu begrenzen. Es liege jetzt an anderen zu entscheiden, ob sie ein Misstrauensvotum vorantreiben wollten. Die Aufsicht über die Verkehrsbehörde hat in Schweden das Infrastrukturministerium. Die bisherige Ministerin Johansson räumte ein, sie habe dabei Fehler gemacht.

Die Oppositionsparteien hatten den Rücktritt aller drei Minister gefordert und zeigten sich unzufrieden, so dass ein Misstrauensvotum für Löfvens Regierung droht, der das Land mit den Grünen seit 2014 in einer Minderheitsregierung mit 138 von 349 Mandaten regiert. Die nächsten Wahlen finden planmäßig im September 2018 statt. Eine oppositionelle bürgerliche Viererallianz (Moderate, Liberale Volkspartei, Christdemokraten und Zentrumspartei) hat bereits ihre Bereitschaft zur Übernahme der Regierungsgeschäfte erklärt. Sie wäre im Parlament allerdings auf die Unterstützung der rechtspopulistischen Schwedendemokraten unter Parteichef Jimmie Åkesson angewiesen (Schwedens Premier Löfven droht Misstrauensvotum,

www.tagesspiegel.de 28.07.2017; Bigalke, Krisenmanager in der Krise, SZ 28.07.2017, 4).

Neuseeland

Domain-Angaben werden besser geschützt

Die neuseeländische Domain Name Commission (DNC) verstärkt ihre Bemühungen um mehr Datenschutz: Mit Wirkung vom 28.11.2017 können natürliche Personen frei wählen, ob ihre Telefonnummer und ihre Adresse im öffentlich einsehbaren WHOIS recherchierbar ist. Voraussetzung ist, dass sie als Verbraucher handeln, also nicht geschäftlich tätig sind. Damit verschwinden sie zwar nicht aus dem WHOIS, sind aber schwerer aufzufinden. Dieser zusätzliche Service muss von allen .nz-Registraren ab spätestens 28.03.2018 angeboten werden. Bis dahin haben das Registry wie auch die Registrare Zeit, ihre Systeme entsprechend umzustellen (Hitzelberger, Neuseeländische-Endung .nz erhält mehr Datenschutz, domain-recht.de 21.06.2017).

USA

FBI warnt vor „intelligentem“ Spielzeug

Das Federal Bureau of Investigation (FBI), die US-Bundespolizei, hat Mitte Juli 2017 eine öffentliche Warnung vor vernetztem Spielzeug ausgesprochen. Smarte Spielsachen und Unterhaltungsgeräte für Kinder, etwa Puppen, Teddybären, Kuscheltiere, beinhalten als sog. „Cloud Pets“ „typischerweise Sensoren, Mikrophone, Kameras, Datenspeicher und andere Multimediafähigkeiten, samt Spracherkennung und GPS. Mit diesen Pets können Sprachnachrichten aufgenommen und abgespielt werden und ermöglichen z. B. entfernt wohnenden Großeltern, den Enkeln Herzensgrüße und Dönnekens von Annodunnemals mitzuteilen. Dies kann aber auch, so das FBI, die Privatsphäre und Sicherheit von Kindern sowie der ganzen Familie gefährden, weil eine große Menge persönlicher Informationen unwissentlich offengelegt werden kann. Ein Mikrophon kann beispielsweise in Hörweite des Geräts geführte Unterhaltungen aufzeichnen und dabei etwa den Namen des Kindes, dessen Schule, Vorlieben und Aktivitäten in Erfahrung bringen. Häufig richten Inhaber Nutzerkonten ein, verraten dabei Name, Geburtsdatum und Adresse und laden bisweilen sogar Bilder hoch. „Darüber hinaus sammeln Firmen große Mengen zusätzlicher Daten, wie Sprachmitteilungen, Unterhaltungen, Bewegungsmuster, die Internet History und IP-Adressen“. Damit steige die Gefahr, dass das Kind Opfer eines Identitätsdiebstahls werde. Auch Kindesmissbrauch werde erleichtert: Ein Angreifer könne sich mit Informationen aus Bildern und Videos, den GPS-Daten und den Vorlieben eines Kindes dessen Vertrauen erschleichen.

Mit der Sicherheit der vernetzten Geräte ist es, so das FBI, oft nicht weit her: „Sicherheitsvorkehrungen für solche Spielsachen können in der Eile, damit auf den Markt zu kommen und sie einfach nutzbar zu machen, übersehen werden“. Und oft erhält nicht nur der Hersteller Zugriff auf sensible Daten, sondern auch dessen Dienstleister, etwa der Betreiber eines Spracherkennungsdienstes. Für Erwachsene, die Kindern trotzdem vernetzte Spielsachen schenken wollen, empfiehlt das FBI: „Informieren Sie sich im Voraus eingehend über bekannt gewordene Sicherheitslücken und lesen Sie das Kleingedruckte. Spielen Sie alle Sicherheitsupdates, sofern verfügbar, ein. Lassen Sie das Gerät nur über vertrauenswürdige Internetzugänge online gehen. Beobachten Sie das Kind beim Spielen genau, wofür manche Spielsachen eine entsprechende Eltern-App anbieten. Achten Sie darauf, dass das Spielgerät komplett ausgeschaltet ist, wenn gerade nicht damit gespielt wird. Sparen Sie mit Ihren Daten und machen Sie bei etwaigen Nutzerkonten nur die minimal erforderlichen Angaben. Diese sichern Sie bitte mit einem starken Passwort, das nicht auch noch anderswo verwendet wird.“ Die Eltern sollten erkunden, mit welcher Verschlüsselung die Daten übermittelt und von den Herstellern aufgezeichnet werden und wie diese beleumundet sind. Der Umstand, dass das FBI erstmals eine solche Warnung aussprach, weist darauf hin, dass die genannten Sicherheitslücken gravierend sind.

In Deutschland sind Geräte wie die Puppe Cayla, so die Bundesnetzagentur im Dezember 2016, die Sprachaufnahmen macht und zwecks Spracherkennung auf einen Server lädt, illegal. Käufer müssen solche Puppen und ähnliche versteckte Spionagegeräte von Rechts wegen „unschädlich machen“ (vgl. DANA 1/2017, 42 ff.; Sokolov, FBI warnt vor vernetztem Spielzeug, www.heise.de 20.07.2017; Graff, Vorsicht! Teddy hört mit, SZ 21.078.2017, 9).

USA

Staubsaugerroboter als Datensammler?

Der US-Hersteller iRobot will die Daten, die seine Roomba-Staubsaugerroboter über die Wohnungen der KundInnen sammelt, an Amazon, Apple oder Google verkaufen. iRobot-Chef Colin Angle erklärte, dass ein derartiger Deal in den nächsten Jahren eingefädelt werden könnte. Die Daten sollten den Markt der Smart-Home-Geräte revolutionieren. Die bei der Reinigungsarbeit gesammelten detaillierten Daten der Wohnungen ermöglichen nicht nur das Erstellen eines Grundrisses, sondern kartieren z. B. genau, wo etwa Sofas und Schränke stehen. Mit diesen Daten könnten etwa smarte Lautsprecher oder Heizungssysteme besser auf die Gegebenheiten eingestellt werden. Angle gesteht ein, dass das große datenschutzrechtliche Fragen aufwerfen dürfte. Er sichert zu, dass sein Unternehmen diese Daten nicht ohne Einwilligung der Nutzenden verkaufen wolle. Die würden dem aber sowieso zustimmen, um ihr Smart Home smarter zu machen.

Robotik-Forscher Guy Hoffman von der Cornell University meint, eine solche Kooperation wäre ein Durchbruch. Gegenwärtig agierten Smart-Home-Geräte noch „wie ein Tourist in New York, der nie die U-Bahn verlässt“. Zwar hätten sie etwas Informationen über ihre Umgebung, aber jede Menge Kontext fehle noch. Die Staubsaugerroboter könnten den liefern helfen. Der Hedge-Fond-Manager Willem Mesdag meint, dass der Ansatz von iRobot dem

der Konkurrenten mit deutlich günstigeren Staubsaugerrobotern überlegen sei: „Die Konkurrenz fokussiert sich darauf, Reinigungsprodukte herzustellen, nicht Roboter, die Karten erstellen." Das könnte den Roombas helfen, weiterhin den Markt zu dominieren. Gleichzeitig geht iRobot aber sowieso auch patentrechtlich gegen die Konkurrenz vor, die teilweise deutlich günstigere Produkte anbietet und die dem großen Vorbild bezüglich der Reinigungsleistung nicht nachstehen (Holland, Roomba: Hersteller der Staubsaugerroboter will Karten der Wohnungen verkaufen, www.heise.de 25.07.2017).

USA

Firma verchipt Beschäftigte

Gemäß eigenen Angaben ist die Firma Three Square Market (32M) die erste US-Firma, die ihre Belegschaft verchipt. Deshalb organisierte sie am 01.08.2017 in River Falls, Wisconsin, eine „Chip Party". Dabei ließen sich die Mitarbeitenden von der dort ansässigen 32M angeblich freiwillig einen winzigen NFC-Chip (Near Field Communication) zwischen Daumen und Zeigefinger einer Hand implantieren.

Der Funkchip soll dann zur drahtlosen Identifikation der Person dienen. In der Folge hofft 32M auf eine große Verbreitung bei tausenden Firmen in aller Welt.

32M-CEO Todd Westby erklärte: „Wir erwarten, dass die RFID-Technik alles vom Bezahlen [in der Kaffeeküche] über das Öffnen von Türen, die Aktivierung von Kopiermaschinen, das Einloggen [...] bis zum Speichern medizinischer Gesundheitsinformationen [...] vorantreiben wird. Eines Tages wird diese Technik standardisiert sein und Ihnen ermöglichen, [den Chip] als Reisepass und Fahrausweis sowie für alle Einkaufsmöglichkeiten und mehr zu nutzen." 32M bietet IT-Systeme und Dienstleistungen für Kleinstgeschäfte in Büros und anderen Arbeitsplätzen. MitarbeiterInnen können dort typischerweise Getränke und Imbisse kaufen und an einer Selbstbedienungskasse bezahlen. Mehr als 2.000 solcher Kioske betreibt 32M derzeit in Europa, Asien, Australien und Nordamerika. Die Schwesterfirma TurnKey Corrections betreibt mehr als 6.000 Kioske in Gefängnissen. 32M hofft, später auch die Mitarbeitenden ihrer Kunden für das Chip-Programm gewinnen zu können. Auch die EndkundInnen von Fitnessstudios und kleinen Lebensmittelgeschäften hat die US-Firma im Visier. Über GefängnisinsassInnen verliert die Verlautbarung kein Wort.

Ideengeber war laut 32M die schwedische Firma BioHax International. Diese Firma aus Helsingborg hat demnach bereits ihre Belegschaft verchipt, so 32M-Manager Patrick McMullan: „Wir freuen uns darauf, mit [BioHax] zusammenzuarbeiten und unseren Marktanteil auf ein anderes Level zu bringen." Die BioHax-Webseite zeigt einen NTAG216-Chip von NXP, der in einer 2 mal 12 Millimeter großen Bioglaskapsel steckt. Laut Herstellerspezifikation speichert der NTAG216 924 Bytes und ist für drahtlose Verbindungen bis zehn Zentimeter Abstand ausgelegt. Pro Sekunde können bis zu 106 kbit übertragen werden. Wie bei RFID üblich, wird auch die zum Betrieb des Chips erforderliche Energie drahtlos übertragen (Sokolov, Chip-Implantat zur Identifikation: Firma will Mitarbeitern Chips einsetzen, www.heise.de 24.07.2017).

USA

Justiz fordert Nutzungsdaten von Trump-GegnerInnen

Das US-amerikanische Justizministerium unter Donald Trump versucht, per Durchsuchungsbefehl persönliche Informationen über BesucherInnen einer regierungskritischen Webseite zu beschaffen. Der Provider Dreamhost sollte zunächst sämtliche Nutzungsdaten wie zum Beispiel die IP-Adresse der Seitenbesucher seiner Kunden weitergeben. Dabei hätte es sich, so Dreamhost, allein um 1,3 Mio. IP-Adressen gehandelt. Der Provider weigerte sich und so landete der Streit mit der Justiz vor dem Superior Court in Washington, D.C. Dort ging am 22.08.2017 nun ein Gerichtsdokument ein, in dem es heißt: „Die Regierung hat kein Interesse an Aufzeichnungen zu den 1,3 Millionen IP-Adressen, von denen in mehreren Pressemitteilungen von Dreamhost zu lesen ist." Herauszugeben seien die Daten der von Dreamhost gehosteten Seite disruptj20.org.

Unter die ursprüngliche Abfrage des Ministeriums wären nicht nur die IP-Adressen gefallen, sondern auch Entwürfe von Blogposts für die Seite und E-Mail-Korrespondenzen der Seitenbesitzer. Dies wurde dem Justizministerium nach eigener Darstellung allerdings erst klar, als Dreamhost sich über die Anfrage beschwerte. Das Justizministerium erklärte daraufhin, es wolle derartige Daten nicht übermittelt bekommen. Man habe bei der Formulierung des Durchsuchungsbefehls schlicht nicht gewusst, wie viele Informationen der Provider Dreamhost habe.

Über die Seite disruptj20.org, die weiterhin Gegenstand der Datenbegehr blieb, waren Proteste gegen die Amtseinführung Trumps organisiert worden. Während der Zeremonie am 20. Januar hatte es landesweit Gegenveranstaltungen gegen den neuen Präsidenten gegeben. Dabei war es am Rande vereinzelt zu Ausschreitungen gekommen. Hunderte Demonstranten müssen sich deshalb nun vor Gericht verantworten. Disruptj20.org unterstützt die Betroffenen mit rechtlichem Beistand.

In der amerikanischen Öffentlichkeit wurde die groß angelegte Datenabfrage zu disruptj20.org als Ermittlung ins Blaue hinein kritisiert. Dreamhost beschwerte sich in einem Blogpost, es sei unklar, was genau den Besuchern der Webseite vorgeworfen werde und ob die Vorwürfe überhaupt eine solche massenhafte Abfrage persönlicher Daten rechtfertigen würden (US-Justiz rückt von massenhafter Datenabfrage ab, www.spiegel.de 23.08.2017).

USA

143 Mio. Equifax-Auskunftei-Datensätze gehackt

Unbekannte Hacker haben bei der US-amerikanischen Auskunftei für Finanzdienstleister Equifax mit Sitz in Atlanta/Georgia wertvolle Daten von bis zu 143 Millionen VerbraucherIn-

nen erbeutet, also von über 40% der US-Bevölkerung. Der Datenklau ist für die Betroffenen besonders gefährlich, weil zu den Daten auch die Sozialversicherungsnummern der Opfer gehören, die in den USA oft zur Identifizierung im Alltag zum Beispiel bei Mobilfunk-Verträgen oder Kreditanfragen genutzt werden. Die Wirtschaftsauskunftei Equifax teilte am 07.09.2017 mit, dass die Angreifer sich in ihrem System auch Zugang zu Namen, Geburtsdaten und Adressen verschafft haben. Die Kombination aus diesen vier Informationen eröffnet Betrügern Tür und Tor zum Identitätsdiebstahl, z. B. um in fremdem Namen Kredite aufzunehmen.

Gemäß Equifax ist die Attacke von Mitte Mai bis Juli 2017 erfolgt. In mehr als 200.000 Fällen seien zudem Kreditkarten-Nummern betroffen und zum Teil auch die Führerschein-Daten, was in US-Amerika ebenfalls oft zur Identifikation genutzt wird. Während aber diese Daten und die Dokumente relativ schnell ausgetauscht werden können, begleitet die Sozialversicherungsnummer eine US-AmerikanerIn üblicherweise ihr gesamtes Leben. Der Vorfall wurde gemäß Firmenangaben am 29.07.2017 bei einer internen Untersuchung festgestellt; die Sicherheitslücke sei sofort geschlossen worden. Equifax machte, im Gegensatz zu anderen ähnlichen Fällen, keine Angaben, ob die Daten durch Verschlüsselung geschützt waren. Etwas später teilte Equifax mit, dass von dem Hack auch Dokumente über Streitigkeiten mit 182.000 KundInnen betroffen sind.

Dieser wurde offensichtlich dadurch möglich, dass es die Firma versäumte, Sicherheitsupdates für eine kritische Lücke zu installieren. Unklar blieb, wie genau die Angreifer ins System gelangten und ob sie an die Gesamtheit der verknüpften Informationen herankommen konnten. Gemäß dem IT-Sicherheitsexperten Helge Husemann von der Firma Malwarebytes hätten die Daten normalerweise getrennt segmentiert aufbewahrt werden müssen, um zu verhindern, dass die verschiedenen Informationen miteinander verknüpft werden können. Angesichts der Dimension des Datendiebstahls sei auch denkbar, dass der Angriff von innen heraus durchgeführt worden sei.

Der Vorfall ließ die Frage aufkommen, weshalb Finanzchef John Gamble und zwei weitere Top-Manager in den ersten August-Tagen Equifax-Aktien im Wert von rund 1,8 Millionen Dollar verkauft haben. Ein Sprecher sagte, sie hätten nur einen geringen Teil ihrer Anteile abgestoßen und zu dem Zeitpunkt nichts von dem Hacker-Einbruch gewusst. Die Equifax-Aktie fiel am der Veröffentlichung folgenden Tag vorbörslich um rund 13%. Diese Optik ist wenig schön, zumal in den zwei Monaten zuvor kein Manager Aktien verkauft hatte. Für sogenannten Insiderhandel, bei dem Aktiengeschäfte auf Basis öffentlich nicht zugänglicher interner Informationen getätigt werden, gibt es in den USA strenge Strafen.

Equifax teilte mit, dass auch einige KundInnen in Kanada und Großbritannien in geringerem Umfang betroffen sind, aus anderen Ländern aber nicht. Man habe die Aufsichtsbehörden informiert und externe Spezialisten mit einer forensischen Prüfung beauftragt. Es sei noch zu früh, die Kosten zu beziffern. Vorstandschef Richard Smith entschuldigte sich bei den betroffenen KundInnen und sprach von einem Schlag, der auf das Herz des Unternehmens gezielt habe. Für Equifax ist der Vorfall besonders unangenehm, weil das Unternehmen selbst Produkte gegen Daten- und Identitätsdiebstahl durch Hacker anbietet. Die Firma fällt nicht zum ersten Mal im Zusammenhang mit Cyber-Attacken auf. Schon 2013 sollen bei Equifax laut Medienberichten Finanzdaten und persönliche Informationen von US-Prominenten entwendet worden sein. Zu den Betroffenen zählten damals unter anderen Beyoncé, Ashton Kutcher und Mel Gibson, aber auch die damalige First Lady Michelle Obama sowie Ex-Vize-Präsident Joe Biden (DANA 2/2013, 73).

Der Umgang von Equifax mit dem aktuellen Angriff sorgte für die Kritik, die Firma habe sich zu lange Zeit mit der Benachrichtigung der Betroffenen gelassen und zu wenige Informationen öffentlich gemacht. Equifax bot den betroffenen US-VerbraucherInnen als versuchte Schadenseindämmung an, sich gebührenfrei bei „Trusted ID“ anzumelden und ein Jahr lang ihre Credit History bei Equifax und dessen Mitbewerbern Transunion und Experian überwachen zu lassen. Dazu kommt eine Kopie des eigenen Equifax Credit Reports, eine Versicherung gegen Identitätsdiebstahl und eine laufende Internetsuche nach der Sozialversicherungsnummer. Die Anmeldung zu Trusted ID verlangte allerdings das Abnicken von Vertragsbedingungen, in denen die Teilnehmenden darauf verzichten, Equifax vor Gericht zu bringen. Auf der Webseite des Unternehmens hieß es dann jedoch: „Die Schiedsgerichtsklausel und der Verzicht auf Sammelklagen in den (Nutzungsbedingungen) bezieht sich nicht auf den (Hack)“. Die erwähnten Klauseln wurden kurz danach entfernt. Der Andrang zu Trusted ID war so groß, dass Equifax Interessierten Anmeldedaten zuteilte und diese auf einen Termin warten mussten, um sich anzumelden. Das Callcenter soll auf mehr als 2.000 TelefonistInnen verdreifacht worden sein.

Derweil äußerten die kanadischen VerbraucherInnen ihren Unmut darüber, dass sie nicht wissen, ob auch ihre Daten preisgegeben wurden. Equifax gäbe nur unter Einschränkungen oder gar nicht Auskunft. Zum Ausmaß der Betroffenen aus Kanada, Großbritannien und Nordirland machte die Firma zunächst keine Angaben. Die Hackerattacke hatte Folgen für das Führungsmanagement. Der Informations- und der Sicherheitschef der Firma wurden mit sofortiger Wirkung in den Ruhestand geschickt.

Gemäß der ab 25.05.2018 geltenden europäischen Datenschutzverordnung müssen die zuständigen Datenschutzbehörden binnen 72 Stunden nach Entdeckung eines Cyberangriffs informiert werden. Carl Leonhard von der IT-Sicherheitsfirma Forcepoint erklärte: „Eine der Lehren ist, dass Unternehmen jederzeit alles Nötige für solche Bekanntmachungen vorhalten müssen.“ Zugleich sei es in den ersten Tagen zunächst oft schwierig, schnell das Ausmaß eines Angriffs einzuschätzen (US-Wirtschaftsauskunftei Equifax meldet große Hacker-Attacke, www.stern.de 08.09.2017; Sokolov, Nach kolossalem Hack bei Wirtschaftsauskunftei: Schiefe Optik bei Equifax, www.heise.de 09.09.2017; Equifax schickt nach Datenklau Führungskräfte in den Ruhestand, www.heise.de 16.09.2017).

China

„Datenschutz-Gesetz“ beeinträchtigt internationale Geschäfte

Bei europäischen Unternehmen in China sorgt ein ab dem 01.06.2017 für die Speicherung sensibler Daten in China eingeführtes neues „Datenschutz-Gesetz“ für Wirbel. Danach dürfen Firmen ab sofort in China gewonnene Daten unter anderem zu Kunden nur noch auf Servern in der Volksrepublik speichern und nicht über die Grenzen ins Ausland transferieren. Die Regierung in Peking argumentiert, Staaten sollten in die Lage versetzt werden, Datenströme zu überwachen, die über ihre Landesgrenzen transferiert werden. Die EU-Handelskammer und die Business Software Alliance mit Sitz in den USA forderten, das Regelwerk müsse überarbeitet werden. Das Gesetz nehme vor allem ausländische Firmen ins Visier. China weist dies zurück. Ausländische Firmen in China fürchten nun, dass ihr Zugang zum Internet gesperrt werde, wenn sie die Regeln nicht befolgten. Der deutsche Werkzeugmaschinenbauer Trumpf bezeichnete das neue Gesetz als die größte Herausforderung für das Geschäft in China, so Tomislav Caleta, IT-Experte des Unternehmens: „Was das Gesetz in Zukunft für unseren Standort in China bedeutet, weiß niemand“. Von dem Gesetz betroffen sein sollen auch Continental und Bosch.

Die EU-Handelskammer äußerte sich besorgt. Die neuen Regelungen zeigten Schwächen und sorgten für Unsicherheiten. In einem Schreiben an die chinesische Internet-Behörde empfiehlt sie eine gründliche Diskussion über das Gesetz. Rechtsanwälte vor Ort erwarten indes nicht, dass die chinesischen Behörden sich davon beeinflussen lassen. Sie setzen vielmehr darauf, dass die Behörden das neue Regelwerk zu Beginn noch nicht allzu strikt anwenden werden. Das prognostiziert unter anderem Barbara Li von der Kanzlei Norton Rose Fulbright. Das Gesetz werde aber auch chinesische Firmen treffen. China setzt darauf, den eigenen Datenraum zu kontrollieren (EU-Handelskammer warnt vor chinesischem Daten-Gesetz, derstandard.at 26.05.2017).

Indien

Supreme Court erkennt Grundrecht auf Privatsphäre an

Nachdem Indiens Supreme Court der Privatsphäre in zwei vorangegangenen Entscheidungen den Status eines Grundrechts abgesprochen hatte, korrigierte er angesichts des großen Biometrieprojekts Aadhaar nun seine Ansicht. Er entschied, dass die Privatsphäre der Bürger für deren Leben und Freiheit immanent ist und von der Verfassung als Grundrecht geschützt wird. Damit wurden zwei Entscheidungen aus den Jahren 1954 und 1961 revidiert, in denen die Privatsphäre noch als nicht verfassungsrechtlich geschützt erklärt wurde. Damals hatten noch Kammern aus zuerst sechs und später acht Richtern entschieden, weswegen nun neun Richter nötig waren, um die alten Urteile zu revidieren. Bei dem Verfahren unterlag die indische Regierung, die die Privatsphäre nur allgemein gesetzlich geschützt sah.

Bei dem Biometrieprojekt Aadhaar werden persönliche Daten zu allen BürgerInnen gesammelt, die sich damit etwa für staatliche Unterstützung anmelden sollen (DANA 3/2016, 150 f.). GegnerInnen bezeichnen das Projekt als Weg hin zu einem „totalitären Staat“, das zugleich zu Datendiebstahl von immensem Umfang einlade. Die Regierung hatte argumentiert, das Recht auf Privatsphäre einer „kleinen Elite“ müsse hinter dem Recht der Masse auf ein würdevolles Leben in einem sich entwickelnden Land zurückstehen. Die neun Richter folgten dieser Argumentation nicht.

Aadhaar war anfangs als freiwillige Datenbank angepriesen worden. In den vergangenen Jahren ist die Teilnahme in immer mehr Bereichen verpflichtend geworden, etwa zur Abgabe der Steuererklärung, um ein Konto zu eröffnen oder sogar für Einkäufe im Wert von mehr als umgerechnet 670 Euro. Die Kläger sahen deswegen die Gefahr, dass der Staat damit allumfassende Profile der Bürger erstellen kann. Wie es jetzt weiter geht, ist noch unklar (Holland, Indiens oberstes Gericht überstimmt sich selbst: Privatsphäre ist doch ein Grundrecht, www.heise.de 24.08.2017).

Nigeria

Internet-Portal zur Korruptionsaufklärung

Nigeria wird zu den Ländern in der Welt gezählt, bei denen Korruption am weistesten verbreitet und etabliert ist. Eine Gruppe von Nicht-Regierungsorganisationen, Kirchenvertretern und der US-Botschaft hat nun ein Internet-Portal ins Leben gerufen, das den Menschen im Land erleichtern soll, Verstöße zu melden. Das Ziel sind nicht die großen Fische, sondern das Bakschisch im Alltag. Auf „Report yourself“ sollen die Staatsbediensteten gemeldet werden, die für ihre Dienste ein zusätzliches privates Entgelt verlangen. Die Seite will damit das Verhalten der Einzelnen anprangern und zu einem Kulturwandel beitragen. Ein Sprecher der Gruppe forderte zudem, dass staatliche Unternehmen wie Wasserversorger ihre Dienste digitalisieren, damit es für korrupte Bedienstete keine Möglichkeit mehr gibt, Geld für sich abzuzweigen.

Bisher galt Korruption in Nigeria als gesellschaftlich akzeptabel oder zumindest als ein Übel, gegen das man nicht ankommt. Wer Bestechung oder Bestechlichkeit bei der Polizei anzeigte, galt als Nestbeschmutzer, weil in fast jeder Familie auch Angestellte des öffentlichen Dienstes zu finden sind, die auch die Hand aufhalten. Seit der Unabhängigkeit vor fast 60 Jahren hat sich jede Regierung den Kampf gegen die Korruption auf die Fahnen geschrieben, passiert ist wenig. Ein detaillierter Bericht der Regierung vom August 2017 versuchte erstmals, Korruption im Land statistisch zu erfassen. Das Amt für Statistik hatte 3.300 Haushalte nach ihren Erfahrungen im Umgang mit offiziellen Stellen befragt und die Angaben auf die ca. 200 Mio. EinwohnerInnen hochgerechnet. Demnach müssen die Menschen durchschnittlich sechs Mal im Jahr Bestechungsgelder zahlen. Wer seinen Führerschein oder die Taxilizenz verlängern möchte, muss oft mehrere Hundert Dollar zahlen. Dies summiert sich nach Berechnungen der Statistikbehörde auf 4,6 Mrd. Dollar. Nigeria, einstmals die größte Volkswirtschaft Afrikas, ist in eine Rezession geschlit-

tert, nachdem der sinkende Ölpreis ein Loch in den Staatshaushalt riss und ein Krieg gegen die Terroristen von Boko Haram und eine Dürre Lebensmittel knapp und teuer machte. Eine der berühmtesten Korrupten im Land ist Diezani Alison-Madueke, früher nigerianische Ölministerin und Chefin der Förderländer-Organisation OPEC. Sie saß viele Jahre direkt an der Quelle und lenkte nach Schätzungen der nigerianischen Economic and Financial Crimes Commission eine halbe Milliarde Dollar in ihre eigenen Taschen (Dörries, Sechs Mal im Jahr Bakschisch, SZ 24.08.2017, 21).

Technik-Nachrichten

Digitale Gedankenerfassung und Datenschutz

Tübinger Forscher um die Neurowissenschaftler Surjo R. Soekadar und Niels Birbaumer sehen große Risiken für den Datenschutz bei Gehirn-Maschine-Schnittstellen und haben in der renommierten Wissenschaftszeitschrift „Science" ethische Richtlinien für den Einsatz von Gehirn-Computer-Schnittstellen formuliert.

Sie halten das Ausspähen von Gedanken für möglich, so Soekadar: „Die technologischen Fortschritte im Bereich der Gehirn-Computer-Schnittstellen entwickeln sich rasant." Schon heute lassen sich beispielsweise, wenn auch nur unter sehr speziellen Bedingungen, der elektronisch gemessenen Hirnaktivität eines Menschen einzelne Worte zuordnen. Bei Facebook erforscht eine ganze Abteilung, wie Anwender bis zu 100 Worte allein mit Gedankenkraft schreiben können. In drei Jahren soll eine entsprechende Schnittstelle auf dem Markt sein.

Wenn Maschinen über spezielle Schnittstellen Hirnsignale eines Menschen lesen können, wirft das bisher wenig diskutierte ethische und rechtliche Fragen auf. Soekadar: „Die neuen Technologien sind eigentlich ein Segen und können beispielsweise das Leben gelähmter Menschen enorm erleichtern." Aber sie bergen auch große Risiken, die rechtzeitig bedacht werden müssten. In ihrem Aufsatz fordern die Forscher unter anderem, dass Hirnsignale, die ein Rechner über Sensoren abgreift, sicher verschlüsselt werden müssen. Nur so könne der Datenschutz gewährleistet und das „Brainhacking", das unbefugte Lesen von Signalen, verhindert werden. Wichtig sei auch, dass Hirnsignale, mit denen Geräte gesteuert werden, in einer elektronischen „Blackbox" aufgezeichnet und für eine begrenzte Zeit gespeichert werden. So könne gegebenenfalls rekonstruiert werden, wer für einen Unfall verantwortlich ist.

Die Forschung in Tübingen zeigt, wie sinnvoll es ist, solche Fragen zu klären. Wenn jemand mit dem von seinem Team entwickelten hirngesteuerten Hand-Exo-Skelett einen Schaden verursachen oder einen Menschen verletzen würde, muss geklärt werden, ob das Kommando für die folgenreiche Bewegung vom Hirn kam oder ein technischer Fehler zugrunde lag. Haftungsrechtlich macht das einen großen Unterschied. Um Unfälle zu verhindern, müsse der Mensch auch jederzeit die Maschine mit Hilfe einer „Veto"-Funktion stoppen können. Soekadars Exo-Skelett lässt sich deshalb mit einer bestimmten Augenbewegung anhalten.

Die Gefahren, die durch Gehirn-Computer-Schnittstellen entstehen, sind für die meisten Menschen derzeit noch weit entfernt. Doch schon jetzt erfassen Fitness-Uhren und Smartphones permanent Daten des menschlichen Körpers, wie etwa Herzfrequenz, Blutdruck, Schlafzyklen oder Bewegungsmuster und übertragen sie an Server irgendwo auf der Welt. Diese Daten könnten von Unternehmen oder Geheimdiensten mit Informationen über Hirnaktivitäten verknüpft und zur Erstellung von sehr genauen Persönlichkeitsprofilen genutzt werden.

Noch problematischer wird es, wenn Hacker über eine Schnittstelle das menschliche Gehirn manipulieren oder sogar kapern könnten. Ein solches „Brainjacking" ist nicht mehr reine Science Fiction. US-Unternehmer Elon Musk hat eine Firma gegründet, die Neuro-Implantate entwickeln soll, die ins menschliche Gehirn gespritzt werden, um es mit künstlicher Intelligenz zu verbinden. Die Leistungen des Gehirns könnten so enorm gesteigert werden. Über solche Schnittstellen ist theoretisch aber auch die Stimulation von außen, der externe und unerlaubte Eingriff in fremde Hirne denkbar. Soekadar warnt vor Panikmache, doch meint er: „Wir wollen, dass die Leute verstehen, was man mit den Daten anstellen kann." Es sei höchste Zeit, über Richtlinien nachzudenken, „damit die Technologien nur zum Nutzen der Gesellschaft eingesetzt und unnötige Risiken vermieden werden" (Janssen, Die Ethik des Gedankenlesens, www.tagblatt.de 07.07.2017).

Rechtsprechung

EGMR

Art. 8 EGMR schützt Arbeitnehmer vor übermäßiger TK-Überwachung

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg hat mit einem ausführlichen Urteil der großen Kammer vom 05.09.2017 – gegen die Stimmen einiger Richter – eine Entlassung wegen privater Internetnutzung am Arbeitsplatz für rechtswidrig erklärt, weil die Überwachung der elektronischen Kommunikation eines Arbeitnehmers eine Verletzung seiner Privatsphäre ist (Az. 61496/08, Barbulescu v. Romania). Diese ist in Art. 8 der Europäischen Menschenrechtekonvention (EMRK) geschützt. Ein Arbeitgeber habe nicht das Recht, das Privat- und Sozialleben seiner Mitarbeitenden am Arbeitsplatz auf Null zu reduzieren. Der Anspruch auf Vertraulichkeit von privater Kommunikation bestehe weiter. Einschränkungen sollten nur so weit gehen wie unbedingt nötig.

Geklagt hatte ein rumänischer Ingenieur, der in seinem Unternehmen für den Verkauf zuständig war. Er hatte über den Internetzugang des Arbeitgebers Nachrichten von seinem Messenger-Konto an seinen Bruder und seine Verlobte verschickt. Es ging darin u. a. um seine Gesundheit und sein Sexualleben. Das Unternehmen hatte die Unterhaltung aufgezeichnet, ohne den Mitarbeiter über die Möglichkeit einer solchen Kontrolle vorab zu informieren. Anfang Juli 2007 kursierte in seinem Unternehmen die Information, einer Kollegin sei wegen privater Internet-Nutzung gekündigt worden. Dies hielt den Mann aber nicht von der Privatkommunikation ab. Mitte Juli legte der Arbeitgeber ihm ein Transkript von 45 Seiten mit der Kommunikation einer Woche vor; die Kündigung folgte. Der Mann klagte gegen seine Entlassung, unterlag aber vor rumänischen Gerichten. Das Unternehmen habe im Rahmen des geltenden Arbeitsrechts gehandelt, und der Ingenieur sei über die Regeln informiert gewesen. Aus Sicht der Straßburger Richter ging die Überwachung jedoch zu weit. Nach dem Urteil soll es Unternehmen zwar möglich bleiben, die Kommunikation von Mitarbeitern zu überprüfen. Allerdings müssen bestimmte Voraussetzungen erfüllt sein, die der Gerichtshof erstmals festlegte.

So muss über die Möglichkeit und das Ausmaß von Kontrollen vorab informiert werden. Außerdem braucht es einen legitimen Grund für die Überwachung. Nicht ausreichend ist der allgemeine Hinweis, das Unternehmen müsse vor Schäden am IT-System geschützt und vor einer Haftung wegen illegaler Online-Aktivitäten bewahrt werden. Die nationalen Gerichte hätten für den Schutz vor Verletzungen des Privatlebens keine ausreichenden Vorkehrungen getroffen. So müsse unterschieden werden, ob lediglich der Kommunikationsfluss aufgezeichnet wird oder auch der Inhalt der Nachrichten, was ein deutlich gravierenderer Eingriff sei. Mildere Kontrollmaßnahmen und weniger einschneidende Konsequenzen als etwa eine Kündigung müssen geprüft werden (siehe die aufgehobene Kammerentscheidung des EGMR vom 12.01.2016, DANA 2016, 36 f.; Entlassung wegen privater Internetnutzung nicht rechtens, www.zeit.de 05.09.2017; Janisch, Gericht stärkt Privatsphäre, SZ 06.09.2017, 21).

EuGH

PNR-Abkommen mit Kanada verstößt gegen Grundrechte

Der Europäische Gerichtshof (EuGH) hat mit einem Gutachten vom 26.07.2017 das Abkommen zum Austausch von Fluggastdaten (Passenger Name Records – PNR) mit Kanada gestoppt (Gutachten 1/15). Mehrere der vorgesehenen Bestimmungen sind nicht mit den von der Europäischen Union anerkannten Grundrechten auf Schutz der Privatsphäre und auf Datenschutz vereinbar. Der EuGH folgte damit der Einschätzung des Generalanwalts Paolo Mengozzi.

Das ab 2010 ausgehandelte und 2014 unterzeichnete Abkommen sieht vor, bis zu 60 Einzeldaten pro Passagier und Flugbuchung fünf Jahre lang zu speichern und an staatliche Stellen in Kanada zu übermitteln. Behörden in Kanada dürfen diese Datensätze auswerten und ohne effektive Kontrolle durch EU-Stellen an weitere Staaten übermitteln. Das Europäische Parlament, das dem Abkommen nach der Unterzeichnung durch den EU-Rat und durch Kanada zustimmen sollte, hatte es dem EuGH im November 2014 zur Prüfung vorgelegt, da es erhebliche Zweifel an dessen Rechtmäßigkeit hatte.

Gemäß dem Gutachten des EuGH würden die weitergegebenen Daten zu viel über die Fluggäste verraten und könnten noch mehr über deren Privatleben preisgeben. Mehrere Bestimmungen des Abkommens beschränkten sich nicht auf das absolut Notwendige und enthalten keine klaren sowie präzisen Regeln. So werden sensible Daten grundrechtswidrig nach Kanada übermittelt. Informationen zu besonderen Mahlzeitwünschen könnten Hinweise auf die Religion oder Erkrankungen geben, etwa dann, wenn Reisende bei der Buchung eine „muslimische Mahlzeit“ oder „glutenfreie Kost“ bestellen. Sensible Daten seien nicht sakrosankt, doch müsse der Umgang damit präzise geregelt werden.

Die Verwendung der Daten auch nach erfolgter Einreise sei nicht hinreichend vor Missbrauch geschützt. Es bedürfe objektiver Kriterien mit materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung durch die kanadischen Behörden. Die Nutzung der Daten bedürfe einer vorherigen Kontrolle durch ein Gericht oder eine unabhängi-

ge Verwaltungsstelle. Eine dauerhafte Speicherung der Daten sei unzulässig. Nur wenn objektive Anhaltspunkte dafür bestehen, dass von bestimmten Fluggästen nach ihrer Ausreise aus Kanada eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzüberschreitender schwerer Kriminalität ausgehen könnte, sei eine Speicherung auch für die Dauer von fünf Jahren zulässig.

Nach Auffassung des Gerichtshofs sind weitere Bestimmungen des geplanten Abkommens nicht mit den Grundrechten vereinbar, so dass das Abkommen geändert werden muss, um die Eingriffe besser und genauer einzugrenzen. Der Gerichtshof stellt dazu fest, dass das Abkommen

- einige der zu übermittelnden PNR-Daten klarer und präziser definieren muss;
- vorsehen muss, dass die im Rahmen der automatisierten Verarbeitung von PNR-Daten verwendeten Modelle und Kriterien spezifisch und zuverlässig sowie nicht diskriminierend sind;
- vorsehen muss, dass nur Datenbanken verwendet werden, die von Kanada im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden;
- vorsehen muss, dass die PNR-Daten von den kanadischen Behörden nur dann an die Behörden eines Nicht-EU-Lands weitergegeben werden dürfen, wenn es ein dem geplanten Abkommen äquivalentes Abkommen zwischen der Union und dem betreffenden Land oder einen Beschluss der Europäischen Kommission in diesem Bereich gibt;
- ein Recht auf individuelle Information der Fluggäste im Fall der Verwendung der sie betreffenden PNR-Datenwährend ihres Aufenthalts in Kanada und nach ihrer Ausreise aus diesem Land sowie im Fall der Weitergabe dieser Daten an andere Behörden oder an Einzelpersonen vorsehen muss;
- gewährleisten muss, dass die Kontrolle der Einhaltung der Regeln für den Schutz der Fluggäste bei der Verarbeitung ihrer PNR-Daten durch eine unabhängige Kontrollstelle sichergestellt wird.

Der Gerichtshof kommt zu dem Schluss, dass das geplante Abkommen in seiner jetzigen Form nicht geschlossen werden durfte. DatenschützerInnen vertraten von Anfang an die Auffassung, dass die EU bei der Speicherung, Nutzung und Verarbeitung sensibler PNR-Daten zu weit geht. Die bereits bestehenden Abkommen mit den USA und Australien sowie die neue EU-Richtlinie zur Fluggastdatenspeicherung müssen nun noch einmal auf den Prüfstand. Die EU-Kommission teilte nach der Verkündung des Gutachtens mit, sie werde alles Erforderliche tun um sicherzustellen, dass der Informationsaustausch fortgesetzt werden kann (EuGH, PE Nr. 84/17 26.07.2017; Holland, EuGH stoppt geplantes Fluggastdaten-Abkommen der EU mit Kanada, www.heise.de 26.07.2017; Steinke, Entscheidung gegen den Generalverdacht, SZ 27.07.2017, 5).

BAG

Anlassloser Einsatz von Keylogger ist unzulässig

Das Bundesarbeitsgericht (BAG) in Erfurt hat am 27.07.2017 letztinstanzlich entschieden, dass der Einsatz eines Software-Keyloggers zur Überwachung eines Arbeitsplatz-Computers nur unter engen Voraussetzungen erlaubt ist (2 AZR 681/16). Nur bei dem mit konkreten Tatsachen belegbaren Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung durch eine konkrete ArbeitnehmerIn darf ein Keylogger eingesetzt werden. In anderen Fällen verstößt die Nutzung der Überwachungssoftware gegen § 32 Abs. 1 Bundesdatenschutzgesetz (BDSG).

Die BAG-Entscheidung bestätigte ein Urteil des Landesarbeitsgerichtes (LAG) Hamm (6 Sa 1711/15). Im konkreten Fall ging es um einen Web-Entwickler in der Bluebox Medienagentur GmbH in Castrop-Rauxel, die auf allen Mitarbeiter-PCs Keylogger installierte und die Belegschaft per E-Mail darüber informierte: „Hallo liebes Team, hiermit informiere ich Euch offiziell, dass sämtlicher Internet-Traffic und die Benutzung der Systeme der Company mitgelogged und dauerhaft gespeichert werden. Solltet Ihr damit nicht einverstanden sein, bitte ich Euch mir dieses innerhalb dieser Woche mitzuteilen.“ Da niemand Widerspruch einlegte, ging die Firma davon aus, dass der Einsatz von Keylogger-Software akzeptiert wäre.

Bei Auswertung der Logfiles wurde festgestellt, dass ein Mitarbeiter den Firmen-PC am 04.05.2015 auch privat nutzte. Noch am selben Tag stellte die Firma den Mitarbeiter frei, der seit vier Jahren in der Firma arbeitete; selbst sein Aprilgehalt erhielt er nicht mehr. Er wurde fristlos entlassen. Insgesamt hatte er drei Stunden seiner Anwesenheitszeit für die Programmierung eines Computerspiels genutzt und 10 Minuten pro Tag die Auftragsverarbeitung des väterlichen Unternehmens gewartet. Bisher habe die Firma es toleriert, dass Mitarbeitende die Computer auch privat nutzen. Die Betroffene entschuldigte sich beim Chef und gelobte Besserung, was diesen aber nicht zum Umdenken bewegte. Der Mitarbeiter machte vor Gericht geltend, nur in den Arbeitspausen programmiert zu haben.

Die Mail, die mit „Hallo liebes Team“ begann, verfolgte anscheinend gezielt den Zweck, den schließlich gekündigten Mitarbeiter auf eine Weise zu überführen, von der er nichts ahnte. Eine Kollegin hatte gemeint, ein paar Wochen zuvor gesehen zu haben, dass dieser seiner Arbeit nicht nachgeht, was sie ihrem Chef meldete. Heimlich war die Überwachung, weil der Bluebox-Chef die Woche nicht abwartete, sondern den Keylogger schon nach 2 Tagen einsetzte.

Das LAG Hamm und zuvor das Arbeitsgericht Herne hatten entschieden, dass der Einsatz eines Keyloggers zur Arbeitskontrolle unverhältnismäßig gewesen sei, weil es mildere Mittel zur Überwachung der Arbeitsleistung gibt. Der BAG-Senatsvorsitzende Ulrich Koch erklärte, dass Mitarbeitende ihr Persönlichkeitsrecht „nicht am Werkstor abgeben“. Der Keylogger der Medienagentur hatte selbst die Kreditkartendaten des Mitarbeiters inklusive Gültigkeitsdauer und Prüfnummer erfasst. Schon zu Beginn der mündlichen Verhandlung hatte sich die Kammer daher zu dem Hinweis genötigt gesehen, „der Kläger möge sich eine neue Kreditkarte besorgen“. Die Tatsache, dass der Einsatz der Software per E-Mail angekün-

digt wurde und niemand Einwände hatte, sei unerheblich, da Schweigen keine Zustimmung sei. Zudem hätte der Arbeitgeber genauer über den Zweck der Datenerhebung wie dem Umfang der Protokollierung informieren müssen.

Auch das BAG sah im Einsatz des Keyloggers eine Verletzung des Rechtes auf informationelle Selbstbestimmung: „Die Beklagte hatte beim Einsatz der Software gegenüber dem Kläger keinen auf Tatsachen beruhenden Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung. Die von ihr ´ins Blaue hinein` veranlasste Maßnahme war daher unverhältnismäßig". In früheren Entscheidungen vor 11 und 12 Jahren hatte das BAG über die „exzessive Privatnutzung" von Dienstrechnern entschieden (Borchers, Bundesarbeitsgericht bestätigt Verwertungsverbot für Keylogger, www.heise.de 27.07.2017; Hipp/Winter, Der Chef als Big Brother, Der Spiegel 31/2017, 128; Esslinger, Mitlesen verboten, SZ 28.07.2017, 2).

KG

Eltern erhalten keinen Zugang zu Facebook-Account der verstorbenen Tochter

Das Kammergericht (KG) in Berlin hat mit Urteil vom 31.05.2017 in zweiter Instanz zu Gunsten von Facebook entschieden, dass eine Mutter zusammen mit dem Kindesvater keinen Zugangsanspruch zu dem Facebook-Account ihres verstorbenen Kindes aus Erbrecht durchsetzen kann (21 U 9/16). Es änderte damit ein Urteil des Landgerichts (LG) Berlin (DANA 1/2016, 40 f.) ab. Der Schutz des Fernmeldegeheimnisses stehe dem Anspruch der Erben entgegen, Einsicht in die Kommunikation der Tochter mit Dritten zu erhalten. Die Tochter war im Alter von 15 Jahren von der U-Bahn erfasst und tödlich verletzt worden. Die Eltern erhofften sich aus den Einträgen in das Facebook-Konto Gewissheit, ob sie sich aus freien Stücken das Leben genommen hat. Facebook verweigerte den Zugriff auf das in den durch die Meldung eines „Freundes" in den „Gedenkzustand" versetzte Konto. Damit können Facebook-„Freunde" Einblick in einstmals geteilte Inhalte nehmen.

Das KG ließ offen, ob die Klägerin und der Kindesvater als Erben in den Vertrag eingerückt seien, den die verstorbene Tochter mit Facebook geschlossen hatte. Es sei zwar grundsätzlich möglich, dass die Erben in die Rechte und Pflichten dieses Vertrages eingetreten seien, und zwar nicht im Sinne der aktiven Fortführung dieses Vertrages, sondern um passive Leserechte zu erhalten. In den von Facebook gestellten Nutzungsbedingungen sei nicht geregelt, ob Rechte aus dem Vertrag im Falle des Todes des Nutzers auf seine Erben übergehen könnten. Auch der Grundgedanke des Vertrages spreche nicht generell dagegen, dass er nicht vererblich sei. Facebook wolle den Nutzern nur eine Kommunikationsplattform zur Verfügung stellen und Inhalte vermitteln. Durch eine Änderung in der Person des Vertragspartners würden die Leistungen in ihrem Charakter nicht verändert.

Doch regele das Bürgerliche Gesetzbuch (BGB) nicht, ob höchstpersönliche Rechtspositionen (ohne vermögensrechtliche Auswirkungen) vererbbar seien. Eine Vererbung setze voraus, dass sie in irgendeiner Form im Eigentum des Verstorbenen verkörpert seien und nicht nur virtuell existierten. Um zu klären, ob es sich bei – nicht verkörperten – E-Mails um solche handele, die aufgrund ihres höchstpersönlichen Inhalts nicht vererbbar seien, oder um solche, die aufgrund ihres wirtschaftlichen Bezuges vererbbar seien, würde man in der Praxis auf erhebliche Probleme und Abgrenzungsschwierigkeiten stoßen.

Das KG entschied aber nicht über die Vererbbarkeit des Facebook-Accounts. Selbst wenn man davon ausgehe, dass dieser Account in das Erbe falle und die Erbengemeinschaft Zugang zu den Account-Inhalten erhalten müsse, stehe das Fernmeldegeheimnis nach dem Telekommunikationsgesetz (TKG) dem Einblick entgegen. Dieses Gesetz sei zwar ursprünglich für Telefonanrufe geschaffen worden. Das Fernmeldegeheimnis werde jedoch in Art. 10 Grundgesetz (GG) geschützt und sei damit eine objektive Wertentscheidung der Verfassung. Daraus ergebe sich eine Schutzpflicht des Staates und auch die privaten Diensteanbieter müssten das Fernmeldegeheimnis achten. Nach einer Entscheidung des Bundesverfassungsgerichts (U. v. 16.6.2009, 2 BvR 902/06, NJW 2009, 2431) erstrecke sich das Fernmeldegeheimnis auch auf E-Mails, die auf den Servern von einem Provider gespeichert seien. Die Nutzenden seien schutzbedürftig, da sie nicht die technische Möglichkeit haben, zu verhindern, dass die E-Mails durch den Provider weitergegeben werden. Dies gelte entsprechend für sonstige bei Facebook gespeicherte Kommunikationsinhalte, die nur für Absender und Empfänger oder jedenfalls einen beschränkten Nutzerkreis bestimmt sind.

Anders als das LG entschieden hat, würden die im vorgesehenen Ausnahmen nicht greifen. Zwar sieht das TKG vor, Dritten Inhalte der Kommunikation zur Kenntnis zu geben, um den Dienst technisch zu ermöglichen oder aufrecht zu erhalten. Da Facebook jedoch seine Dienste nur beschränkt auf die Person des Nutzers anbiete, verbiete der Schutz der weiteren Beteiligten an den Kommunikationsvorgängen (Chats) die Kenntnisgabe.

Es gäbe auch keine andere gesetzliche Vorschrift, die eine Ausnahme vom Schutz des Fernmeldegeheimnisses macht (sogenanntes „kleines Zitiergebot"). Das Erbrecht nach dem BGB zielte nicht darauf ab, das Fernmeldegeheimnis einzuschränken. Auch aus sonstigen Gründen sei es nicht geboten, ohne gesetzliche Regelung Ausnahmen zuzulassen und von dem so genannten „kleinen Zitiergebot" abzuweichen.

Es läge auch darin kein Verzicht auf den Schutz des Fernmeldegeheimnisses, dass, worauf sich die klagende Mutter berief, die Tochter ihr die Zugangsdaten überlassen hat. Dieser Umstand war zwischen den Parteien streitig. Ein solcher Verzicht hätte durch alle diejenigen erfolgen müssen, die in einem Zwei-Personen-Verhältnis mit der Verstorbenen kommuniziert haben.

Das KG verneinte zudem, dass die Klägerin außerhalb des Erbrechts einen Anspruch auf Zugang zu dem Account hat. Das Recht der elterlichen Sorge verhelfe nicht zu einem solchen Anspruch, da es mit dem Tode des Kindes erlösche. Das den Eltern noch zufallende Totenfürsorgerecht könne nicht dazu dienen, einen Anspruch auf Zugang zu dem Social-Media-Account des verstorbenen Kindes herzuleiten. Auch das eigene Persönlich-

keitsrecht der Mutter sei nicht geeignet, einen Anspruch auf diesen Zugang zu begründen. Als ein Teilbereich des Persönlichkeitsrechts sei z. B. anerkannt, seine eigene Abstammung zu kennen. Trotz des verständlichen Wunsches der Eltern, die Gründe für den tragischen Tod ihres Kindes näher zu erforschen, lasse sich hieraus kein Recht auf Zugang zu dem Account ableiten. Auch wenn eine verbleibende Unkenntnis darüber die Persönlichkeitsentfaltung der Eltern massiv beeinträchtigen könne, gebe es auch vielfältige andere Ereignisse, die die gleiche Wirkung zeigen könnten. Dadurch würde das allgemeine Persönlichkeitsrecht zu einem konturenlosen und nicht mehr handhabbaren Grundrecht führen. Der vorsitzende Richter des KG Björn Retzlaff erklärte, ihnen sei als Gericht die Entscheidung nicht leicht gefallen. Eine Änderung der Rechtslage könne nur durch den Gesetzgeber erfolgen. Das KG hat die Revision zum Bundesgerichtshof zugelassen (Kammergericht: Urteil zu Lasten der klagenden Mutter - kein Zugriff der Eltern auf Facebook-Account ihrer verstorbenen Tochter, PM 30/2017 31.05.2017; Janisch, Letzte Unruhe, SZ 01.06.2017, 8).

NdsOVG

Weitgehende ÖPNV-Videoüberwachung in Hannover zugelassen

Das Niedersächsische Oberverwaltungsgericht (NdsOVG) hat mit Urteil vom 07.09.2017 die Berufung der Landesbeauftragten für den Datenschutz Niedersachsen (LfD Nds.) gegen ein Urteil des Verwaltungsgerichts (VG) Hannover zurückgewiesen und damit die Aufhebung einer datenschutzrechtlichen Anordnung im Ergebnis bestätigt (Az. 11 LC 59/16).

Die klagende ÜSTRA hat in zahlreichen ihrer Fahrzeuge feststehende Videokameras installiert, mit denen im sog. Blackbox-Verfahren durchgehend Bewegtbilder vom Fahrzeuginnenraum aufgezeichnet werden. Die Videosequenzen werden nach 24 Stunden wieder gelöscht. Die Aufzeichnung dient unter anderem zur Beweissicherung bei Vandalismusschäden und zur Verfolgung von Straftaten. Die Datenschutzbehörde in Hannover gab der ÜSTRA im August 2014 mit einer auf § 38 Abs. 5 BDSG gestützten Verfügung auf, die Videoüberwachung in ihren Bussen und Stadtbahnen während des Einsatzes der Fahrzeuge im öffentlichen Personennahverkehr einzustellen und erst wieder aufzunehmen, nachdem sie entweder ein Konzept für einen nach Linien und Zeit differenzierten Einsatz der Videotechnik erarbeitet und umgesetzt hat oder anhand konkreter Anhaltspunkte darlegt, dass die Videoüberwachung zeitlich und örtlich unbeschränkt erforderlich ist. Sie wollte die Rund-um-die-Uhr-Aufzeichnung in den Bussen und Bahnen wegen eines fehlenden Nachweises der Wirksamkeit unterbinden. Nach ihrer Einschätzung bietet die Videoaufzeichnung in Hannover von Kriminalität betroffenen Fahrgästen nur scheinbar Schutz. Denn anders als bei einer Kameraüberwachung, bei der wie bei der Braunschweiger Straßenbahn eine Leitstelle das Geschehen beobachtet und eingreifen kann, bewirkten die Kameras in Hannover nur eine Scheinsicherheit, die den Erwartungen der Fahrgäste nach mehr Sicherheit durch eine Videoüberwachung nicht gerecht wird. Eine Videoaufzeichnung rund um die Uhr sei nur dann gerechtfertigt, wenn etwa über Ermittlungserfolge nachgewiesen werden könne, dass diese bei der Aufklärung oder Vermeidung von Straftaten und Vandalismus hilft.

Die ÜSTRA hingegen hatte wie die Landesnahverkehrsgesellschaft Niedersachsen von einer abschreckenden Wirkung durch die Kameras gesprochen, die schwer mit Zahlen zu belegen sei. ÜSTRA-Sprecher Udo Iwannek: „Die Ermittlungsbehörden kennen zahlreiche Fälle, wo aufgrund von unseren Videoaufnahmen Straftäter gefasst werden konnten. Gerade vor dem Hintergrund der gegenwärtigen Bedrohungslage, auch mit Blick auf mögliche Terroranschläge, scheint uns ein Abschalten von Videotechnik der vollkommen falsche Weg zu sein.“ Eine Live-Überwachung sei aber technisch zu aufwändig.

Der gegen die Verfügung gerichteten Klage hatte das VG Hannover mit Urteil vom 10.02.2016 (Az. 10 A 4379/15) mit der Begründung stattgegeben, das BDSG sei nicht anwendbar, weil die ÜSTRA eine öffentliche Stelle des Landes Niedersachsen sei, für die der Datenschutz durch Landesgesetz geregelt sei (DANA 2/2016, 109). Das niedersächsische Datenschutzgesetz (NDSG) enthalte keine Eingriffsermächtigung, auf die die Verfügung der Landesdatenschutzbeauftragten gestützt werden könnte.

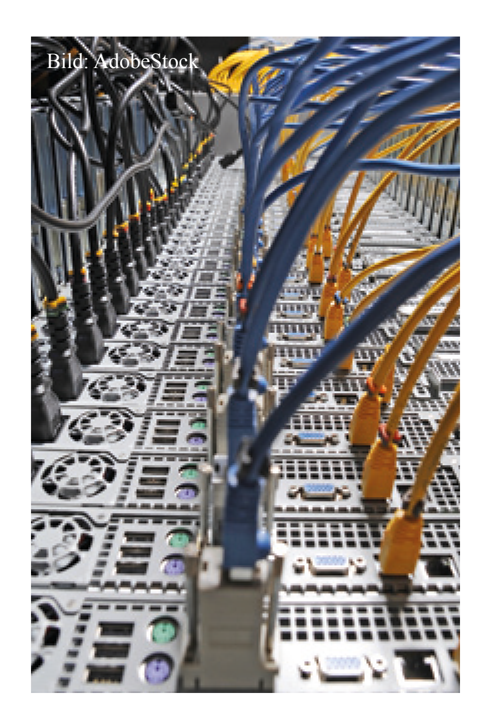
Das NdsOVG bestätigte die Entscheidung des VG im Ergebnis. Zwar sei das BDSG anwendbar; doch erlaube dieses der ÜSTRA die Videoüberwachung in ihren Fahrzeugen. Die Videoüberwachung diene der Wahrnehmung berechtigter Interessen der ÜSTRA, insbesondere der Verfolgung von Straftaten gegen ihre Einrichtungen und der Verhütung solcher Straftaten. Die erforderliche Abwägung mit den schutzwürdigen Interessen des von den Überwachungsmaßnahmen betroffenen Personenkreises falle zugunsten der von der ÜSTRA geltend gemachten Belange aus.

Die Revision zum Bundesverwaltungsgericht hat der 11. Senat nicht zugelassen (OVG lässt Videoüberwachung im Nahverkehr in Hannover zu, www.welt.de 07.09.2017; PM OVG Lüneburg 07.09.2017, Videoüberwachung in den Stadtbahnen und Bussen der ÜSTRA ist mit dem Datenschutzrecht vereinbar; Datenschützer scheitern mit Klage gegen Kameraüberwachung in Bus und Bahn, www.heise.de 09.09.2017).

OVG Münster

TK-Vorratsdatenspeicherung wird ausgesetzt

Das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen in Münster hat die neu in Deutschland geregelte Vorratsspeicherung von Telekommunikations- (TK-) Verbindungsdaten mit Beschluss vom 22.06.2017 wenige Tage vor Beginn ihrer Gültigkeit für europarechtswidrig erklärt (Az. 13 B 238/17). Das Ende 2015 in Kraft getretene Gesetz schreibt Zugangsanbietern vor, ab dem 01.07.2015 Verbindungsinformationen ihrer KundInnen zehn Wochen und Standortdaten einen Monat lang zu speichern. Der Beschluss beruht auf einem einstweiligen Rechtsschutzverfahren, das der Münchner Zugangsanbieter Spacenet initiierte. In der ersten Instanz hatte das Verwaltungsgericht (VG) Köln Anfang des Jahres den


Bild: AdobeStock

vorläufigen Rechtsschutz abgelehnt. Der OVG-Beschluss erging ohne mündliche Verhandlung und ist nicht anfechtbar. Ein Gang zum Bundesverfassungsgericht im Hauptsacheverfahren oder zum Europäischen Gerichtshof bleibt möglich.

Die vorgeschriebene Speicherpflicht erfasst pauschal die Daten nahezu aller NutzerInnen von Telefon- und Internetdiensten. Der EuGH hatte mit Urteil vom 21.12.2016 in Bezug auf Schweden und Großbritannien, wo Speicherpflichten für 6 bzw. 12 Monate vorgesehen waren, entschieden, dass eine Vorratsdatenspeicherung von vornherein auf Fälle beschränkt werden muss, „bei denen ein zumindest mittelbarer Zusammenhang mit der durch das Gesetz bezweckten Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit besteht“. Dies könne etwa durch personelle, zeitliche oder geographische Kriterien geschehen. Die anlasslose Speicherung der Daten könne nicht dadurch kompensiert werden, dass Behörden nur zum Zweck der Verfolgung schwerer Straftaten beziehungsweise der Abwehr schwerwiegender Gefahren Zugang zu den gespeicherten Daten erhalten. Auch strengere Maßnahmen zum Schutz der gespeicherten Daten vor Missbrauch würden insoweit nicht ausreichen. Auch der Wissenschaftliche Dienst des Bundestags diagnostizierte einen Verstoß gegen EU-Recht. Wenige Tage nach der Gerichtsentscheidung, am 28.06.2017, setzte daraufhin die Bundesnetzagentur die Pflicht zur Umsetzung der Massenspeicherung vorerst aus (Heidrich/Holland, Oberverwaltungsgericht: Vorratsdatenspeicherung ist europarechtswidrig, www.heise.de 22.06.2017 Janisch, Vorratsspeicherung vorerst ausgesetzt, Ausgebremst, SZ 29.06.2017, 1, 6).

AG Bad Hersfeld

Telefonnummern-Weitergabe an WhatsApp setzt Einwilligung voraus

Das Amtsgericht (AG) Bad Hersfeld entschied mit Beschluss vom 20.03.2017 in einem familiengerichtlichen Sorgerechtsstreit, dass die automatische Weitergabe von Telefonnummern von Kontakten an WhatsApp, ohne die Betroffenen vorher um Erlaubnis zu fragen, rechtswidrig ist (F 111/17 EASO). Im konkreten Fall ging es um die Smartphone-Nutzung eines elf Jahre alten Jungen. Das Gericht erlegte dabei der Mutter konkrete Auflagen zur elterlichen Kontrolle der Smartphone-Nutzung ihres Kindes auf. Der Beschluss verpflichtet die Mutter, von allen Personen, die aktuell im Adressbuch des Smartphones ihres Sohnes gespeichert sind, schriftliche Zustimmungserklärungen einzuholen, dass diese mit der Weitergabe an WhatsApp einverstanden sind. Zudem wurde der Mutter eine persönliche Weiterbildung zur digitalen Mediennutzung aufgetragen.

Der Junge hatte zum Geburtstag ein eigenes Smartphone bekommen und dieses nach Auffassung der Eltern exzessiv genutzt. Auf dem Gerät gespeichert waren über 20 Kontakte, darunter Familienangehörige, Mitschüler, Freunde und Nachbarskinder. Laut Geschäftsbedingungen von WhatsApp ist die Nutzung erst ab dem 13. Lebensjahr gestattet.

Datenschützer sehen bereits seit geraumer Zeit einen Rechtsverstoß darin, dass WhatsApp nach der Zustimmung des Anwenders zu den Allgemeinen Geschäftsbedingungen automatisch auf sämtliche im Smartphone gespeicherten Kontakte zugreift, egal ob diese selbst WhatsApp nutzen oder nicht. Die für andere Gerichte nicht bindende Entscheidung des Amtsgerichts hatte „Signalwirkung“ und löste eine Debatte aus. Rechtsanwalt Christian Solmecke: „Viele Menschen werden jetzt erst auf die seit Jahren gängige Praxis des Unternehmens aufmerksam.“

Der Amtsrichter in Bad Hersfeld verwies auf die bestehende Abmahngefahr: Wer durch seine Nutzung von WhatsApp „diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden“.

Der Stuttgarter Medienrechtler Carsten Ulbricht hält die Entscheidung für falsch. Ein privater Nutzer von WhatsApp könne nicht dafür verantwortlich gemacht werden, dass das Programm im Hintergrund alle gespeicherten Kontakte herunterlade. Im persönlichen und familiären Bereich seien bestimmte Regelungen des Datenschutzgesetzes ausdrücklich nicht anzuwenden. Der Einsatz von WhatsApp könne nicht einmal als „fahrlässig“ bezeichnet werden, da die Nutzer von der Datenweitergabe nichts wüssten. Im Ergebnis irrt Ulbricht: Die Rechtswidrigkeit ergibt sich nicht aus dem Datenschutzrecht, sondern aus der zivilrechtlichen Verletzung des allgemeinen Persönlichkeitsrechts. Und es ist zweifellos fahrlässig, ein IT-Gerät zu nutzen, mit dem das Persönlichkeitsrecht Dritter verletzt wird. Diese Funktionalitäten von WhatsApp müssen jedem, der den Dienst nutzt, bekannt sein.

Ulbricht weist zudem darauf hin, dass das geringe Abmahnrisiko für private Nutzende nicht auf den geschäftlichen Bereich übertragen werden kann. Insofern sind die rechtlichen Rahmenbedingungen enger. Die Nutzung von WhatsApp könnte zu Konflikten mit dem Gesetz führen. Solmecke sieht das ähnlich und empfiehlt Berufsgruppen wie Versicherungsvertretern oder Bankberatern, die auf ihrem Smartphone Kundendaten gespeichert haben, den Dienst vorerst nicht auf ihrem beruflichen Gerät zu installieren (Weitergabe von Kontaktdaten an WhatsApp unzulässig, www.zeit.de 27.06.2017; Nau, Amtsgericht: Weitergabe von Kontaktdaten an WhatsApp unzulässig, www.swp.de 28.06.2017).

Buchbesprechungen

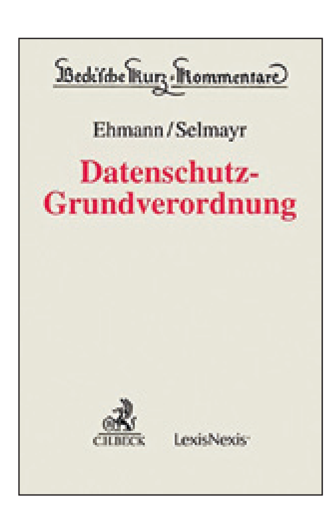


Bergmann, Lutz/Möhrle, Roland/Herb, Armin
Datenschutzrecht
Boorberg Stuttgart,
52. Ergänzungslieferung, März 2017

(tw) Das Elend von Loseblattsammlungen zum Datenschutzrecht besteht derzeit darin, dass die Rechtsänderungen aktuell mit einer Geschwindigkeit erfolgen, dass eine geordnete Fortschreibung des früheren Rechts kaum möglich ist. Vor dieser Herausforderung kapituliert aber der „Bergmann/Möhrle/Herb“ (BMH) nicht, sondern versucht, aus der Not eine Tugend zu machen, indem er sukzessive das neue Recht zum Einordnen bringt. Das gelingt dem BMH auch, indem er den Text und die Erwägungsgründe der europäischen Datenschutz-Grundverordnung (DSGVO) schon im Mai 2016 eingefügt und inzwischen einige Artikel der DSGVO (Art. 1, 2, 28, 32, 35, 36, 59) kommentiert hat. Hierbei nehmen die ursprünglichen Autoren, von denen Lutz Bergmann 2012 verstorben ist, die Unterstützung weiterer Autoren in Anspruch und zwar der Anwälte Jens Eckhardt und Ralph Wagner.

Der Vorteil der Loseblattsammlung besteht darin, dass das gesamt Gesetzesrecht im Zugriff ist, was weiterhin gilt, und manches kommentiert auf aktuellem Niveau. So ist beim BMH etwa schon der neue § 6b BDSG zur Videoüberwachung erläutert. Im Hinblick auf die kommenden Regelungen sind dem gegenüber aber die gebundenen Kommentare mit vielen Autoren im Vorteil. Dies verschärft sich nun dadurch, dass neben dem alten in der nächsten Ergänzungslieferung auch noch das neue BDSG kommentiert werden muss. Dort, wo die Ergänzungen vorgenommen werden, sind sie auf dem neuesten Stand, auch im Hinblick auf aktuelle Urteile z. B. des Europäischen Gerichtshofs.

Wer also darauf angewiesen ist, die aktuellen Datenschutzregelungen in Deutschland im schnellen Zugriff zu haben und wer aussagekräftige Kommentierungen mit weiteren Hinweisen sucht, ohne in jedem Fall auf dem neuesten Stand zu sein, der ist weiterhin mit dem Bergmann/Möhrle/Herb gut bedient. Was dieser nicht leisten kann, ist die gesamte Breite der Datenschutzdiskussion zeitnah zu begleiten. Der im Jahr 1977 begründete Kommentar hat schon viele Datenschutzstürme überstanden. Es ist ihm zu gönnen, dass er trotz der gewaltigen gebundenen Konkurrenz auch den Wechsel zur DSGVO konstruktiv und informativ bewältigt.



Ehmann, Eugen/Selmayr, Martin (Hrsg.)
Datenschutz-Grundverordnung,
C.H.Beck München, 2017,
ISBN 978-3-406-70215-0, 1243 S., 139 €.

(tw) Nach Paal/Pauly, Kühling/Buchner und Gola wirft der C. H. Beck-Verlag mit dem Ehmann/Selmayr die vierte Kommentierung zur Datenschutz-Grundverordnung (DSGVO) in die juristische Diskussion. Das mit über 1200 Seiten etwas ungenau als „Kurz-Kommentar“ beworbene Werk macht den Überblick über die Auslegung der DSGVO nicht einfacher, gibt aber Einblicke, die in den bisherigen Werken zu kurz kommen.

Dies ist insbesondere dem Umstand zuzuschreiben, dass einige der Autoren ganz nah am Entstehungsprozess der DSGVO beteiligt waren als Vertreter des Parlaments, der Kommission, der Bürokratie in Brüssel oder in den Mitgliedstaaten oder als Wirtschaftslobbyisten. Hinzu kommen einige Wissenschaftler mit gutem Namen und einige Rechtsanwälte: J. P. Albrecht, U. Baumgartner, N. Bertermann, M. Braun, H. Heberlein, J. Hladjk, H. G. Kamann, A. Klabunde, R. Knyrim, T. Kranig, S. Mentel, P. Nemitz, A. Paschke, B. Raum, S. Schiedermair, A. Schiff, M. Schweinoch, R. Selk, M. Will, T. Zerdick – also buchstäblich von A bis Z keine Unbekannten in der Diskussion über den Datenschutz. Der Herausgeber Martin Selmayr sitzt als Kabinettschef des EU-Kommissionspräsidenten in Brüssel im Zentrum der Macht und war in dieser Funktion vom Anbeginn bis zur Verabschiedung der DSGVO eingebunden; sein Partner Eugen Ehmann hatte schon die Vorgängerregelung, die EG-Datenschutzrichtlinie kommentiert. Dass die Nähe zur Macht auch informationshindernd sein kann, zeigt sich bei der Suche nach dem EU-US-Privacy Shield, das im Stichwortverzeichnis gar nicht vorkommt und dem als Datenschutzschild vier unkritische gedruckte Zeilen gewidmet sind.

Die Diskussionsnähe zum DSGVO-Entstehungsprozess bringt es mit sich, dass der Kommentar insbesondere für die europarechtlich-wissenschaftliche Sichtweise neue Erkenntnisse bringt,

die sich gegenüber der eher praxisorientierten nationalen Sichtweise der meisten anderen Werke heraushebt. Das Problem auch dieses Kommentars – wie von allen des Beck-Verlags – ist, dass hinsichtlich der inhaltlichen Positionen keine klare Linie erkennbar ist, so dass verarbeitungs- neben grundrechtsfreundlichen, meinungsstarke und neben eher deskriptiven Interpretationen abgedruckt sind. Durchgängig ist dagegen die hervorragende europarechtliche Fundierung mit vielen Verweisen auf die Rechtsprechung der europäischen Gerichte, insbesondere des Europäischen Gerichtshofs, sowie auf die Aussagen der Art. 29-Arbeitsgruppe und die Referenz v. a. zur deutschsprachigen Literatur, soweit sie bis Anfang 2017 erschienen ist. Trotz der eher wissenschaftlichen Ausrichtung des Kommentars gibt er auch wertvolle Hinweise für die praktische Auslegung und Umsetzung der DSGVO.



Sydow, Gernot (Hrsg.)
Europäische Datenschutzgrundverordnung – Handkommentar
Nomos Verlag Baden-Baden 2017,
ISBN 978-3-8487-1782-8, 1456 S., 128,00 €

(tw) Nachdem der Beck-Verlag den Markt schon stark abgegrast hat (mit Paal/Pauly, Kühling/Buchner, Gola und Ehman/Selmayr, dazu s. o.) und der Otto-Schmidt-Verlag mit der Zweitauflage des Plath ins Rennen um die Gunst der an der Datenschutz-Grundverordnung (DSGVO) Interessierten einstieg, sind nun auch der Auernhammer-Kommentar des Heymanns-Verlags und der „Sydow“ von Nomos verfügbar. Nomos hatte zuvor schon mit Monografien von Albrecht/Jotzo, Laue/Nink/Kremer und Roßnagel die ganz frühen Interessenten abgedeckt und kann nun mit einem umfassenden „Handkommentar“ zur DSGVO aufwarten. Anders als Plath und Auernhammer konzentriert sich der Sydow auf die DSGVO und nimmt nicht noch das alte – inzwischen überarbeitete – Bundesdatenschutzgesetz mit auf. Angesichts der Verfügbarkeit alter Kommentare zum alten BDSG ist dies kein Nach-, sondern eher ein Vorteil.

Handlich kann der „Handkommentar“ nur durch enge Schrift und dünnes Papier sein. Tatsächlich behandelt der „Sydow“ die DSGVO sehr umfassend und mit einer erfreulichen Tiefe. Sowohl der Herausgeber wie auch die 21 weiteren AutorInnen aus Wissenschaft, Anwaltschaft und ein wenig richterlicher bzw. ministerieller „Praxis“ (Kampert, Greve) sind bisher in der Datenschutzliteratur noch nicht so stark präsent. Das ändert aber nichts daran, dass auch dieser Kommentar von hoher handwerklicher Qualität ist, aber leider auch Kinderkrankheiten anderer Werke aufweist, was wohl auch dem noch fehlenden Praxisbezug zuzuschreiben ist. Auch wenn er nicht so umfangreich Literaturhinweise (bis Mai 2017) enthält wie andere Kommentare, findet man zu allen der vielen wesentlichen Auslegungsfragen der DSGVO eine fundierte Darstellung und Diskussion. Ähnlich wie bei den anderen auf dem Markt verfügbaren Werken lässt sich nicht sagen, dass hier eine eher datenschutzfreundliche- oder datenschutzkritische Position überwiegt; die Darstellung ist insofern unterschiedlich, aber durchgängig sachlich und nüchtern und stark an den praktischen Anwendungsbedürfnissen und weniger an wissenschaftlicher Diskussion interessiert.

Der oder die für die DSGVO Interessierte steht vor dem Dilemma, dass der Kommentarmarkt redundant mit durchgängig brauchbaren Angeboten bestückt ist. Hinsichtlich des Preis-Leistungsverhältnisses schneidet dabei der „Sydow“ ganz gut ab, zumal er zwar teurer als der Gola, aber auch substanzreicher ist. Weitere Werke werden erscheinen. Auch wenn es noch keine Rechtsprechung zur DSGVO gibt, Meinungen sind schon viele auf dem Markt; die Diskussionen haben begonnen. Dadurch, dass das neue BDSG von juristischen Skrupeln weitgehend unberührt blieb, wird der Markt und die Diskussion weiterhin geflutet werden und werden müssen.



Schantz, Peter/Wolff, Heirich Amadeus
Das neue Datenschutzrecht
Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis
C.H.Beck 2017,
ISBN 978 3 406 69649 7, 417 S., 59 €

(tw) Die schon sehr umfassende Literatur zur Datenschutz-Grundverordnung (DSGVO) in Kommentaren, Fachaufsätzen und Monografien beginnt, das Ende Juni 2017 im Bundesgesetzblatt veröffentlichte Bundesdatenschutzgesetz (BDSG) mit zu berücksichtigen. Der Beck-Verlag hat es nun geschafft, keine zwei Monate nach der Veröffentlichung des neuen BDSG eine systematische Darstellung des deutschen Datenschutzrechtes auf den Markt zu bringen, in der das neue nationale Recht vollständig einbezogen wird. Dafür gewonnen hat er den zuständigen Fachreferenten im Bundesjustizministerium Schantz sowie den Universitätsprofessor mit dem Schwerpunkt Datenschutz Wolff. Herausgekommen ist eine gut leserliche, informative und kompetente Darstellung des deutschen Datenschutzrechts mit seinen umfassenden europarechtlichen Grundlagen. Zwar wird der Schwerpunkt auf die DSGVO gelegt, doch kommen auch die e-Privacy-Richtlinie

mit dem umsetzenden deutschen Recht sowie die Richtlinie für Justiz und Inneres mit ihrer Konkretisierung in den §§ 45 ff. BDSG nicht zu kurz.

Ausgangspunkt für die systematische Darstellung ist das grundsätzliche europäische Recht, bei dem die nationalen Regelungen dann jeweils mit eingeblendet, dargestellt und erläutert werden. Dabei werden, ausgehend vom Verfassungsrecht und von der Geschichte, zunächst die Grundprinzipien und die Zulässigkeit der Verarbeitung, dann die technisch-organisatorischen Pflichten, die Durchsetzung des Rechts und besondere Verarbeitungssituationen abgearbeitet. Praktisch nicht behandelt wird das bereichsspezifische nationale Datenschutzrecht. Die Darstellung nimmt umfassend Bezug auf die vorliegende EuGH-Rechtsprechung und selektiv auf Veröffentlichungen in der Literatur. Zu kurz kommt die kritische Sicht der Rechtslage, was vielleicht bei einem Ministeriumsmitarbeiter und einem oft für die Bundesregierung tätigen Professor auch nicht überraschen mag. Wenn auch verfassungswidrige Passagen des BDSG unreflektiert durchgewunken werden, so wird zumindest das ferner liegende EU-US-Privacy Shield kritisch bewertet. Ausführlich befasst sich Schantz mit dem Verbot automatisierter Einzelentscheidungen; relativ kurz kommt – wie fast durchgängig bei juristischen Publikationen – der technische Datenschutz.

Instruktiv sind die fachlichen Erläuterungen, Tabellen (z. B. mit einem Vergleich JI-Richtlinie und DSGVO) und die historischen Fallbeschreibungen. Das Ganze wird umrahmt durch eine nachvollziehbare Gliederung, ein recht umfangreiches Literaturverzeichnis sowie ein Sachregister. Will sich jemand neu in das Rechtsgebiet einarbeiten und gleich auf dem neuesten Stand sein, so ist das Buch gut geeignet. Auch zur ersten Beantwortung von detaillierten Einzelfallfragen gibt das Werk handbuchartig nützliche Hinweise. Wer tiefer bohren will, bekommt zwar viele gute Anregungen und Hinweise, doch genügt die Darstellung dann nicht mehr, insbesondere, wenn gegen den Strich gebürstet werden soll.



Buchner, Benedikt (Hrsg.)
Datenschutz im Gesundheitswesen
Loseblatt, 13. Lfg. 7/2017, AOK-Verlag, ISBN 978-3-553-43000-5.

(tw) Einrichtungen, die mit Gesundheitsdaten zu tun haben, haben es hinsichtlich der Wahrung des Datenschutzes und der zumeist zusätzlich geltenden Berufsgeheimnisse nicht leicht: Die einzuhaltenden Regelungen strotzen nicht gerade in Bezug auf Klarheit und Übersichtlichkeit. Dies ist einer der Gründe für die vorliegende Loseblattsammlung, die inzwischen zum 13. Mal ergänzt wurde. War diese bei ihrem ersten Erscheinen noch recht unvollständig und unübersichtlich (DANA 2/2012, 98), so ist dieses Problem weitgehend behoben. Die beiden Schnellordner sind inzwischen prall gefüllt mit praktischen Ratschlägen insbesondere für Datenschutzbeauftragte von Gesundheitseinrichtungen. Ihre Struktur ist sowohl pädagogisch wie systematisch begründet, beginnend mit den rechtlichen Grundlagen und den Aufgaben der Datenschutzbeauftragten, und arbeitet dann spezifische Einzelthemen ab: Informationstechnologie, Krankenhaus, gesetzliche Krankenversicherung (noch sehr dünn), Arztpraxis, Rehabilitation, Pflege. Am Ende werden die übergreifenden spezifischen Themen Beschäftigtendatenschutz und Risiko-/Compliance-Management behandelt sowie eine immer weiter aus Tätigkeitsberichten von Aufsichtsbehörden bestückte Fallsammlung von A-Z, also von „amtsärztlicher Untersuchung“ bis „Zugriffsberechtigung – Notzugriff“ und informationstechnischen Grundbegriffen. Glossar, Literaturverzeichnis und Index runden das Ganze ab.

Das Konzept, eine einfache verständliche, aber hinreichend tiefgehende und detaillierte Darstellung vorzunehmen, ohne sich über in der Wissenschaft ausgetragene Streitfragen auszulassen und entsprechende Verweise vorzunehmen, wurde beibehalten und erweist sich als praxisgerecht. Der Medizindatenschutz ist komplex genug, dass weiterhin einige wenige Lücken bleiben, wobei aber inzwischen der Gesamtüberblick erkennbar ist. Die Datenschutz-Grundverordnung ist natürlich – was bei einem Loseblattwerk mittelfristig unmöglich ist – noch nicht umfassend eingearbeitet, findet aber inzwischen ebenso Eingang wie neue technische Entwicklungen, mit denen sich die Praxis herumschlagen muss wie z. B. das IT-Sicherheitsgesetz, die Angebote von Facebook oder Google oder der WLAN-Einsatz oder so abseitig erscheinende, aber real anfallende Fragen wie Videodolmetschen oder Whistleblowing.



Münch, Florian
Autonome Systeme im Krankenhaus
Datenschutzrechtlicher Rahmen und strafrechtliche Grenzen
Nomos, Baden-Baden 2017, 369 S.
ISBN 978-3-11-048562-2

(tw) Wenn in der von Eric Hilgendorf und Suanne Beck herausgegebenen Reihe „Robotik und Recht“ eine Dissertation mit dem Titel „Autonome Systeme im Krankenhaus“ veröffentlicht wird, dann macht das neugierig, insbesondere wenn im Untertitel der Datenschutz auftaucht. Zwar gibt es massenhaft Publikationen zum Thema „Big Data“ und „Künstliche Intel-

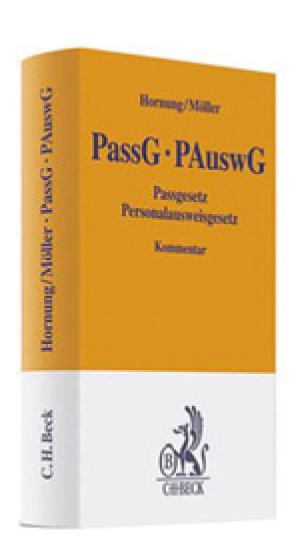
ligenz" und das auch im Bereich des Gesundheitswesens, doch bleiben die Texte zumeist an der Oberfläche und legen nicht den Schwerpunkt auf das Recht und den Datenschutz. Der Grund für diesen Mangel ist evident: Zwar ist digitale Medizin gerade ein medialer Hype, doch im Detail wird es rechtlich und technisch hochkompliziert.

So darf man auch nicht allzu enttäuscht sein, wenn die Erwartungen an eine umfassende und grundlegende Behandlung von der vorliegenden Arbeit nicht vollständig erfüllt werden. Münch beschreibt zunächst einige Erscheinungsformen, Praktiken und einzelne Anwendungen der Robotik im Gesundheitsbereich und setzt sich dann mit den rechtlichen Grundlagen der ärztlichen Schweigepflicht und des Datenschutzes auseinander. Dabei macht er nicht den Fehler, ausführlich die Genese der rechtlichen Instrumente zu behandeln, er versäumt es aber, in Bezug auf den Medizinbereich deren Schutzgüter genauer zu bestimmen, was für eine Behandlung des Gesamtthemas wünschenswert gewesen wäre. Er stellt seine Ausführungen unter das Hauptthema „Autonomie" und erwähnt dabei nur beiläufig, dass Schweigepflicht und Datenschutz einen erheblich umfassenderen Ansatz verfolgen, die neben den individuellen Schutzgütern auch gesellschaftliche Werte einschließen und die nicht nur abstrakt Autonomie, sondern auch konkret Diskriminierungsschutz und Gesundheitsschutz zum Ziel haben.

Der Hauptteil der Arbeit besteht darin, dass sie die datenschutzrechtlichen Instrumente des BDSG anhand des Einsatzes „autonomer Systeme" im Krankenhaus durchdekliniert. Dabei orientiert sich der Autor sehr dogmatisch an der Terminologie des BDSG und greift nicht die moderneren Ansätze der Datenschutzgrundverordnung (DSGVO) auf. Dies wäre zumindest in Ansätzen möglich gewesen, auch wenn die Arbeit im Januar 2015 abgeschlossen wurde, als die Diskussion über die DSGVO noch in vollem Gange war. Ein Anknüpfen z. B. an den Grundprinzipien der DSGVO hätte evtl. zur Folge gehabt, dass die Risikoorientierung des Datenschutzrechts sowie organisatorische und technische Erwägungen ausführlicher behandelt worden wären. So wird die Technik zunächst sehr formal unter dem Stichwort „Datensicherheit" abgehandelt, um dann an anderer Stelle richtig, aber zu knapp und unvermittelt technische Lösungen zu darzulegen. Organisatorische Ansätze wie Standardisierungen, Zertifizierungen oder Verhaltensregeln werden nicht behandelt. Systematisch knüpft die Darstellung an Regelungen und nicht an konkreten Robotikanwendungen an, was dazu führt, dass diese nicht ganzheitlich unter die Lupe genommen werden. Themen, die bisher regulativ nur am Rande behandelt werden, wie z. B. Fragen der Protokollierung oder der Algorithmen-Kontrolle werden nicht so vertieft, wie es angesichts der bei Big-Data-Verfahren auftretenden Problematik angemessen gewesen wäre.

Einige behandelte Themen werden ausführlich behandelt, obwohl sie in der Praxis keine größere Bedeutung haben. So stellt sich die Haftungsfrage bei der medizinischen Robotik weniger nach dem Datenschutzrecht hinsichtlich immaterieller Schädigungen, sondern im Hinblick auf materielle Verletzungen, die über § 823 reguliert sind. Bei der Diskussion über Robotikeinsätze sollte es nicht darum gehen, wie Haftungsansprüche oder Strafbarkeit rechtlich vermieden werden können, sondern welche Regulierungen nötig sind, um eine Verletzung zentraler Schutzgüter zu vermeiden. Die Genauigkeit der Sensorik hat in der Praxis keine Relevanz für die Frage der Anonymisierung bzw. Datensparsamkeit. Die Frage der Zweckbindung steht nicht im Zentrum der durch sog. künstliche Intelligenz verursachten rechtlichen Fragestellungen. Die Big-Data-Fragestellungen lassen sich nicht auf die Auswertung von sog. Meta-Daten reduzieren.

Auch wenn einzelne Ausführungen in der Arbeit weniger überzeugend sind, so sind die am Ende dargestellten Lösungsansätze zielführend. Der Versuch, bei einem derart im Wandel befindlichen wie dem vorliegenden Thema, zu dem es noch keine vertiefte Diskussion gibt, eine umfassende Behandlung vorzunehmen, kann wohl auch nicht vollständig gelingen. Der Verdienst des Autors besteht darin, diesen Versuch gestartet und dabei einige wichtige Aspekte behandelt zu haben.



Prof. Dr. Gerrit Hornung, Jan Möller
Passgesetz, Personalausweisgesetz – Kommentar
Verlag C. H. Beck, München,
1. Auflage, 2011
ISBN 978 3 406 61579 5

(sh) Einen Kommentar für das deutsche Pass- und Personalausweisrecht in einer Datenschutzzeitschrift zu rezensieren, das erscheint nur auf den ersten Blick ungewöhnlich, denn mit der Einführung von elektronischen Komponenten zur Speicherung biometrischer Daten in Pässen und Personalausweisen hat sich das Bundesinnenministerium vielfältiger Kritik aus Datenschützerkreisen ausgesetzt. Es muss also aufhorchen lassen, wenn der Verlag C. H. Beck diese Materie über weite Strecken aus der Feder des Passauer Hochschullehrers Gerrit Hornung bearbeiten lässt. Der Kommentator fällt seit einigen Jahren als aufstrebender Akademiker aus der Schule von Prof. Alexander Roßnagel in der Datenschutzszene positiv auf. Die damit verbundene Erwartung wird nicht enttäuscht: Das 2011 erstmalig erschienene Werk widmet sich mit Beiträgen beider Autoren erfreulich ausführlich den aktuellen datenschutzrechtlichen Fragestellungen, die mit den elektronischen Komponenten in Pässen und Personalausweisen und ihrer Herstellung und Verwendung verbunden sind. Die Autoren widmen sich daran anschließend auch kundig den bürgerrechtlich brisanten Passentziehungen z.B. gegen (mutmaßliche) Hooligans und stellen diese in den Kontext des Gefahrenabwehrrechts, unter erfreulich umfangreicher Beleuchtung von Rechtsprechung

und Literatur auf aktuellem Stand.

So rückt der Kommentar nicht etwa nur für Behörden und Insider relevante Fragen in den Vordergrund, sondern stellt sich der datenschutz- und bürgerrechtlichen Problematik des Ausweiswesens. Er erschließt dabei die Verwaltungsvorschriften, praktische Bezüge zur Informationstechnik, zu den Datenbanken der Sicherheitsbehörden und zu europarechtlichen Vorgaben und widmet sich den häufigen Parallelen zum Aufenthalts- und Staatsangehörigkeitsrecht. Dazu zitieren die Autoren verbreitete Fachzeitschriften oder liefern zu gerichtlichen Entscheidungen die Geschäftszeichen und Entscheidungsdaten, mit denen sie zumeist leicht aufzufinden sind. Diese Herangehensweise würde man sich auch für andere Kommentierungen des besonderen Verwaltungsrechts wünschen.



Prof. Dr. Nikolaus Forgó,
Prof. Dr. Marcus Helfrich,
Prof. Dr. Jochen Schneider:
Betrieblicher Datenschutz,
C.H.Beck, 2017, 1331 S.,
ISBN 978-3-406-69541-4, 209,-- €

(wh) Aller guten Dinge sind drei, heißt es. Das gilt dann hoffentlich auch für die dritte Auflage dieses Werkes. Allerdings ist dieses Werk dieses Jahr gerade in der zweiten Auflage erschienen. Der Titel „Betrieblicher Datenschutz" weckt Erwartungen, die das Werk nicht erfüllt, nämlich, dass es alle Aspekte des betrieblichen Datenschutzes abdeckt. Dazu gehören auch die Regelungen zum Beschäftigtendatenschutz und die zur Pflicht zur Benennung betrieblicher Datenschutzbeauftragter. Diese Erwartung kann das Werk nicht erfüllen, da es hierzu einige Monate zu früh erschienen ist. Das Vorwort zu dieser 2. Auflage datiert vom April 2017. Das Bundesdatenschutzgesetz (BDSG-neu), das am 25. Mai 2018 gleichzeitig mit dem Gültigwerden der EU-Datenschutzgrundverordnung (DSGVO) in Kraft tritt, konnte noch nicht in der vom Bundesrat und Bundestag beschlossenen Fassung berücksichtigt werden. Es wird zwar an der einen oder anderen Stelle auf den politischen Willen der deutschen Politik verwiesen, mehr aber auch nicht. Im Gegenzug werden aber an vielen Stellen noch die Regelungen des derzeitigen BDSG (BDSG-alt) umfangreich erläutert, die zum Zeitpunkt des Schreibens dieser Rezension gerade noch acht Monate gültig sein werden.

Abgesehen davon ist das Konzept dieses Werkes sehr gut gelungen, sich nicht an der DSGVO entlang zu hangeln, sondern eine Strukturierung anhand der Themen des betrieblichen Datenschutzes vorzunehmen. Nach einer Darstellung der allgemeinen datenschutzrechtlichen Grundlagen und Strukturen im Teil I werden alle relevanten Themen des betrieblichen Datenschutzes dargestellt. Dies geht von der Datenschutzorganisation über Themen wie „Archivierung und Entsorgung", „Datenschutz in Betrieb, Unternehmen und Konzern", „Outsourcing und neue Technologien als Herausforderung für den Datenschutz" und dem „Konfliktmanagement im Datenschutz" bis hin zur den Regelungen zu Bußgeldern und Strafen.

Das Kapitel „Betrieblicher Datenschutzbeauftragter" ist genauso wie das Kapitel „Beschäftigtendatenschutz" leider unvollständig und für die praktische Umsetzung im betrieblichen Alltag nicht ausreichend. Ohne eine Erörterung der Regelungen aus dem BDSG-neu ist das Wissen um die Regelungen der DSGVO in diesen beiden Gebieten nur ungenügend dargestellt. Hier ist es wesentlich zu wissen, wie die Konkretisierungsklauseln, die der europäische Gesetzgeber den Nationalstaaten hier eingeräumt hat, ausgefüllt worden sind. Im Kapitel „Datenschutz in der Telekommunikation" werden die Regelungen des Telekommunikationsgesetzes (TKG) in Bezug zur DSGVO gesetzt und dargestellt. Aber selbst im Abschnitt „Perspektiven" dieses Kapitels fehlt jeglicher Hinweis auf den am 10. Januar 2017 von der EU-Kommission veröffentlichten Entwurf der ePrivacy-Verordnung (ePrivVO), die die derzeit auf EU-Ebene gültige EU-ePrivacy-Richtlinie (ePrivRL) ablösen soll. Es wird nur von der Erforderlichkeit der Anpassung nationaler Regelungen an die DSGVO gesprochen. Zwar sind die Datenschutzregelungen im TKG die nationale Umsetzung vieler Regelungen der ePrivRL und damit auch nach dem Gültigwerden der DSGVO solange gültig, bis die ePrivRL durch die ePrivVO abgelöst wird und die Datenschutzregelungen des TKG durch die direkt geltende ePrivVO verdrängt werden. Aber da nach der derzeitigen Planung die ePrivVO gleichzeitig mit der DSGVO gültig werden soll, wäre bei diesem Werk, dessen Vorwort im April 2017 geschrieben worden ist, zumindest eine ausführliche Erwähnung des ePrivVO-Entwurfs nicht nur erwartbar, sondern auch zwingend erforderlich gewesen. Auch wird zwar im Kapitel „Adresshandel" richtig festgestellt, dass die Anforderungen des § 7 Abs. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) weiterhin zu beachten sind (vgl. Teil 10, Kapitel 1, Rn 82), da diese von der DSGVO nicht berührt werden. Eine Herleitung dieser Aussage wird nicht angegeben. Es fehlt jeglicher Hinweis darauf, dass der § 7 UWG auch der Umsetzung von Art. 13 der ePrivRL in Deutschland dient und auch eine datenschutzrechtliche Regelung ist, die nicht von der DSGVO verdrängt wird.

Die Inhalte dieses Werkes lassen sich durch ein ausführliches Inhaltsverzeichnis und ein sehr umfangreiches Stichwortverzeichnis gut erschließen.

Fazit: Interessierte Leserinnen und Leser sollten – gerade bei dem nicht unerheblichen Preis für dieses Werk – besser auf die dritte Auflage warten, in der dann hoffentlich das BDSG-neu ausführlich erörtert ist und die ePrivVO – sofern sie beim Erscheinen der dritten Auflage noch nicht verabschiedet sein sollte – zumindest in angemessener Weise erwähnt wird. Die derzeit vorliegende Ausgabe wird leider am 25. Mai 2018 bereits in einigen Teilen veraltet sein, und wesentliche Informationen, die für die Umsetzung des betrieblichen Datenschutzes bereits jetzt im Hinblick auf den 25. Mai 2018 benötigt werden, fehlen leider noch. Deshalb kann die dritte Auflage mit Spannung erwartet werden, da in dieser diese Mängel beseitigt sein sollten.

„Datenschutz ist schön, aber in Krisenzeiten wie diesen hat Sicherheit Vorrang“

Thomas de Maizière in den Tagesthemen vom 22.03.2016



Die Wahrscheinlichkeit, bei einem Autounfall zu sterben, ist in Deutschland über 1000 mal größer als durch einen Terroranschlag.